

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-069548

(43)Date of publication of application : 07.03.2003

(51)Int.Cl.

H04L 9/08  
G06F 15/00  
G10K 15/02

(21)Application number : 2001-251689

(71)Applicant : SONY CORP

(22)Date of filing : 22.08.2001

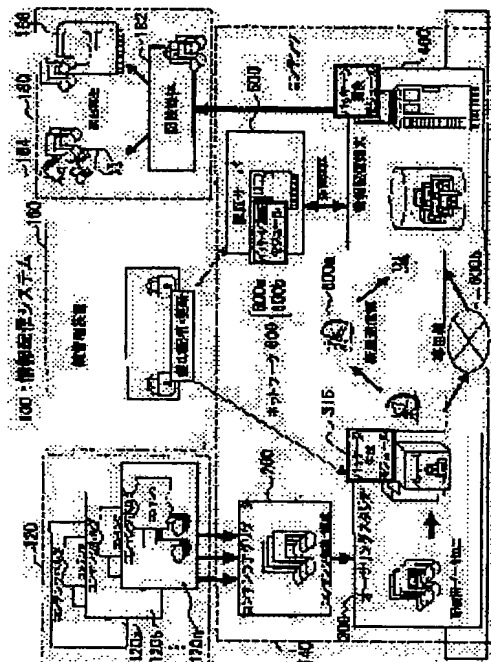
(72)Inventor : YOSHITOMI KAZUNORI  
YOSHINO KENJI  
UENO SHINICHI

(54) AUTHORIZING SYSTEM, AUTHORIZING KEY GENERATION DEVICE, AUTHORIZING DEVICE, AUTHORIZING METHOD, COMPUTER PROGRAM, AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an information distribution system capable of preventing unauthorized copying.

SOLUTION: The invention is an authorizing system that conducts authorizing by encryption for copyright protection for content data distributed via an information distribution terminal 400. An authorizing key generating device 160 generates a content identifier (CID) uniquely allocated to each content data, an authorizing key usage key (CEK) uniquely allocated to each authorizing device that conducts authorizing for content data, a content key (Kc) used in encryption of content data, and an authorizing key (CED) obtained from encryption of a second content key (EKc) using CID and CEK. The second content key (EKc) is derived from encryption of the content key by a root key (Kroot). An authorizing device 316 is provided with a decrypting means for decrypting CED to get Kc and EKc using CID and CEK, and an encryption means for encrypting content data using the decrypted Kc to generate an authored and encrypted content data (E (Kc, Content)).



## LEGAL STATUS

[Date of request for examination]

20.02.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-69548

(P2003-69548A)

(43) 公開日 平成15年3月7日 (2003.3.7)

(51) IntCl.

識別記号

F I

チーゴト (参考)

H04L 9/08

G06F 15/00

330Z

5B085

G06F 15/00

830

G10K 15/02

5J104

G10K 15/02

H04L 9/00

601D

601E

審査請求 未請求 請求項の数30 O L (全 26 頁)

(21) 出願番号

特願2001-251689(P2001-251689)

(22) 出願日

平成13年8月22日 (2001.8.22)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 吉高 和憲

東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(72) 発明者 吉野 賢治

東京都品川区北品川6丁目7番35号 ソニ  
ー株式会社内

(74) 代理人 100095957

弁理士 亀谷 美明 (外3名)

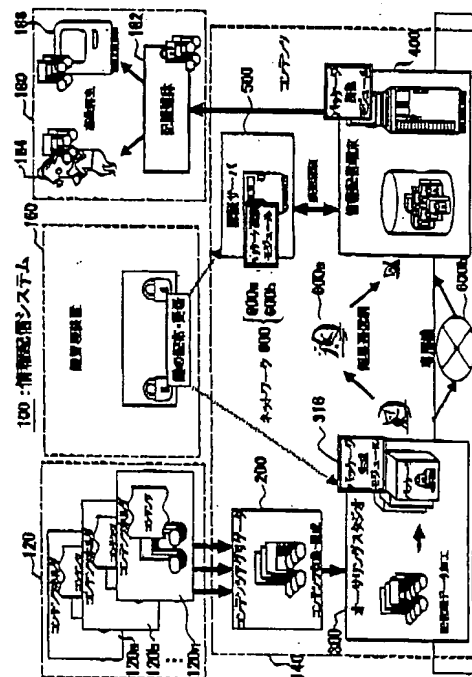
最終頁に続く

(54) 【発明の名称】 オーサリングシステム、オーサリング鍵生成装置、オーサリング装置、オーサリング方法、コンピュータプログラムおよび記憶媒体

(57) 【要約】

【課題】 不正コピーを防止可能な情報配信システムを提供する。

【解決手段】 情報配信端末400を介して配信するコンテンツデータに著作権保護の暗号化を施してオーサリングするオーサリングシステムである。オーサリング鍵生成装置160は、コンテンツデータ毎にユニークに割り当てられるコンテンツ識別子 (CID) と、コンテンツデータをオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、コンテンツデータを暗号化するコンテンツ鍵 (Kc) およびコンテンツ鍵をルート鍵 (Kroot) で暗号化した第2のコンテンツ鍵 (EKc) をCIDおよびCEKを用いて暗号化したオーサリング鍵 (CED) とを生成する。オーサリング装置316は、CEDから、CIDとCEKを用いてKcとEKcとを復号化する復号化手段と、復号化したKcを用いてコンテンツデータを暗号化し、オーサリングされた暗号化コンテンツデータ (E (Kc, Content)) を生成する暗号化手段と備えている。



(2)

特開2003-69548

1

2

## 【特許請求の範囲】

【請求項1】 情報配信端末を介して配信するコンテンツデータ (Content) に対して著作権保護の暗号化を施してオーサリングするオーサリングシステムであって：前記コンテンツデータ (Content) 毎にユニークに割り当てられるコンテンツ識別子 (CID) と、コンテンツデータ (Content) をオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、前記コンテンツデータ (Content) を暗号化するコンテンツ鍵 (Kc) および前記コンテンツ鍵をルート鍵 (Root) で暗号化した第2のコンテンツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) とを生成するオーサリング鍵生成装置と；前記オーサリング鍵 (CED) から、前記コンテンツ識別子 (CID) と前記オーサリング鍵使用鍵 (CEK) を用いて、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) とを復号化する復号化手段と、復号化した前記コンテンツ鍵 (Kc) を用いて前記コンテンツデータ (Content) を暗号化し、オーサリングされた暗号化コンテンツデータ (E (Kc, Content)) を生成する暗号化手段と備えたオーサリング装置と；から成ることを特徴とする、オーサリングシステム。

【請求項2】 前記オーサリング装置は、前記暗号化手段によって得られる暗号化コンテンツデータ (E (Kc, Content)) と、前記コンテンツ識別子 (CID) と、前記第2のコンテンツ鍵 (EKc) とを一つのパッケージデータとしてパッケージ化するパッケージ手段をさらに備えることを特徴とする、請求項1に記載のオーサリングシステム。

【請求項3】 前記コンテンツ鍵 (Kc) は、前記第2のコンテンツ鍵 (EKc) と前記ルート鍵 (Root) から得られる鍵であって、前記暗号化コンテンツデータ (E (Kc, Content)) を復号可能とし、前記ルート鍵 (Root) をセキュアに保持する再生装置において前記コンテンツデータ (Content) を再生可能とすることを特徴とする、請求項1に記載のオーサリングシステム。

【請求項4】 前記ルート鍵 (Root) は、前記再生装置に関連するデバイス鍵 (Kdevice) により暗号化されたコンテンツ使用可能化鍵 (EKB) に組み込まれて保持されており、前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) に加えて前記コンテンツ使用可能化鍵 (EKB) も暗号化されていることを特徴とする、請求項3に記載のオーサリングシステム。

【請求項5】 前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (E

Kc) に加えてチェックサム情報も暗号化されていることを特徴とする、請求項1に記載のオーサリングシステム。

【請求項6】 前記オーサリング鍵 (CEK) の更新があった場合には、更新前のオーサリング鍵 (CEK) の破棄を行う破棄手段をさらに備えることを特徴とする、請求項1に記載のオーサリングシステム。

【請求項7】 前記コンテンツデータ (Content) は、メインコンテンツデータとメインコンテンツデータの付加情報とから成ることを特徴とする、請求項1に記載のオーサリングシステム。

【請求項8】 情報配信端末を介して配信するコンテンツデータ (Content) に対して著作権保護の暗号化を施してオーサリングするためのオーサリング鍵を生成するオーサリング鍵生成装置であって：前記コンテンツデータ (Content) 毎にユニークに割り当てられるコンテンツ識別子 (CID) と、前記コンテンツデータ (Content) をオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、前記コンテンツデータ (Content) を暗号化するコンテンツ鍵 (Kc) および前記コンテンツ鍵をルート鍵 (Root) で暗号化した第2のコンテンツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) とを生成することを特徴とする、オーサリング鍵生成装置。

【請求項9】 前記コンテンツ鍵 (Kc) は、前記第2のコンテンツ鍵 (EKc) と前記ルート鍵 (Root) から得られる鍵であって、前記暗号化コンテンツデータ (E (Kc, Content)) を復号可能とし、前記ルート鍵 (Root) をセキュアに保持する再生装置において前記コンテンツデータ (Content) を再生可能とすることを特徴とする、請求項8に記載のオーサリング鍵生成装置。

【請求項10】 前記ルート鍵 (Root) は、前記再生装置に関連するデバイス鍵 (Kdevice) により暗号化されたコンテンツ使用可能化鍵 (EKB) に組み込まれて保持されており、前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) に加えて前記コンテンツ使用可能化鍵 (EKB) も暗号化されていることを特徴とする、請求項8に記載のオーサリング鍵生成装置。

【請求項11】 前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) に加えてチェックサム情報も暗号化されていることを特徴とする、請求項8に記載のオーサリング鍵生成装置。

【請求項12】 前記オーサリング鍵 (CEK) の更新があった場合には、更新前のオーサリング鍵 (CEK) の破棄を行う破棄手段をさらに備えることを特徴とする

(3)

特開 2003-69548

3

4

る、請求項 8 に記載のオーサリング鍵生成装置。

【請求項 13】 情報配信端末を介して配信するコンテンツデータ (Content) に対して著作権保護の暗号化を施してオーサリングするためのオーサリング鍵を生成するオーサリング鍵生成装置であって：コンピュータを、前記コンテンツデータ (Content) 毎にユニークに割り当てられるコンテンツ識別子 (CID) と、前記コンテンツデータ (Content) をオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、前記コンテンツデータ (Content) を暗号化するコンテンツ鍵 (Kc) および前記コンテンツ鍵をルート鍵 (Kroot) で暗号化した第 2 のコンテンツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) とを生成するオーサリング鍵生成装置として機能せしめることを特徴とするコンピュータプログラム。

【請求項 14】 情報配信端末を介して配信するコンテンツデータ (Content) に対して著作権保護の暗号化を施してオーサリングするためのオーサリング鍵を生成するオーサリング鍵生成装置であって：コンピュータを、前記コンテンツデータ (Content) 毎にユニークに割り当てられるコンテンツ識別子 (CID) と、前記コンテンツデータ (Content) をオーサリングするオーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、前記コンテンツデータ (Content) を暗号化するコンテンツ鍵 (Kc) および前記コンテンツ鍵をルート鍵 (Kroot) で暗号化した第 2 のコンテンツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) とを生成するオーサリング鍵生成装置として機能させるコンピュータプログラムが格納されたコンピュータ読み取り可能な記憶媒体。

【請求項 15】 情報配信端末を介して配信するコンテンツデータ (Content) に対して著作権保護の暗号化を施してオーサリングするオーサリング装置において：前記コンテンツデータ (Content) を記憶するコンテンツ記憶手段と；前記コンテンツデータ (Content) 毎にユニークに割り当てられるコンテンツ識別子 (CID) と、前記オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、前記コンテンツデータ (Content) を暗号化するコンテンツ鍵 (Kc) および前記コンテンツ鍵をルート鍵 (Kroot) で暗号化した第 2 のコンテンツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) と、から成る鍵情報を記憶する鍵情報記憶手段と；前記オーサリング鍵 (CED) か

ら、前記コンテンツ識別子 (CID) と前記オーサリング鍵使用鍵 (CEK) を用いて、前記コンテンツ鍵 (Kc) と前記第 2 のコンテンツ鍵 (EKc) とを復号化する復号化手段と前記コンテンツ鍵 (Kc) を用いて前記コンテンツデータ (Content) を暗号化して暗号化コンテンツデータ (E (Kc, Content)) を生成する暗号化手段と、を備えることを特徴とする、オーサリング装置

【請求項 16】 さらに、前記暗号化手段によって得られる暗号化コンテンツデータ (E (Kc, Content)) と、前記コンテンツ識別子 (CID) と、前記第 2 のコンテンツ鍵 (EKc) とを一つのパッケージデータとしてパッケージ化するパッケージ手段と：を備えることを特徴とする、請求項 15 に記載のオーサリング装置。

【請求項 17】 前記オーサリング鍵 (CED) は、前記パッケージデータ作成装置とは別体に構成された権限のあるオーサリング鍵生成装置において暗号化されることを特徴とする、請求項 15 に記載のオーサリング装置。

【請求項 18】 前記コンテンツ鍵 (Kc) は、前記第 2 のコンテンツ鍵 (EKc) と前記ルート鍵 (Kroot) から得られる鍵であって、前記暗号化コンテンツデータ (E (Kc, Content)) を復号可能とし、前記ルート鍵 (Kroot) をセキュアに保持する再生装置において前記コンテンツデータ (Content) を再生可能とすることを特徴とする、請求項 15 に記載のオーサリング装置。

【請求項 19】 前記ルート鍵 (Kroot) は、前記再生装置に関連するデバイス鍵 (Kdevice) により暗号化されたコンテンツ使用可能化鍵 (EKB) として保持されており、前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第 2 のコンテンツ鍵 (EKc) に加えて前記コンテンツ使用可能化鍵 (EKB) も暗号化されていることを特徴とする、請求項 18 に記載のオーサリング装置。

【請求項 20】 前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第 2 のコンテンツ鍵 (EKc) に加えてチェックサム情報も暗号化されていることを特徴とする、請求項 15 に記載のオーサリング装置。

【請求項 21】 前記オーサリング鍵 (CEK) の更新があった場合には、更新前のオーサリング鍵 (CEK) の破棄を行う破棄手段をさらに備えることを特徴とする、請求項 15 に記載のオーサリング装置。

【請求項 22】 前記コンテンツデータ (Content) は、メインコンテンツデータとメインコンテンツデータの付加情報とから成ることを特徴とする、請求項 15 に記載のオーサリング装置。

【請求項 23】 前記パッケージ手段は、さらに前記コ

(4)

特開 2003-69548

5

6

ンテンツデータ (Content) に関する付加情報であるフリンジデータを合わせてパッケージ化することを特徴とする、請求項15に記載のオーサリング装置。

【請求項24】 情報配信端末を介して配信するコンテンツデータ (Content) に対して著作権保護の暗号化を施してオーサリングするオーサリング装置において：コンピュータを、前記コンテンツデータ (Content) を記憶するコンテンツ記憶手段と；前記コンテンツデータ (Content) 毎にユニークに割り当てられるコンテンツ識別子 (CID) と、前記オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、前記コンテンツデータ (Content) を暗号化するコンテンツ鍵 (Kc) および前記コンテンツ鍵をルート鍵 (Root) で暗号化した第2のコンテンツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) と、から成る鍵情報を記憶する鍵情報記憶手段と；前記オーサリング鍵 (CED) から、前記コンテンツ識別子 (CID) と前記オーサリング鍵使用鍵 (CEK) を用いて、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) とを復号化する復号化手段と前記コンテンツ鍵 (Kc) を用いて前記コンテンツデータ (Content) を暗号化して暗号化コンテンツデータ (E (Kc, Content)) を生成する暗号化手段と、して機能せしめることを特徴とするコンピュータプログラム。

【請求項25】 情報配信端末を介して配信するコンテンツデータ (Content) に対して著作権保護の暗号化を施してオーサリングするオーサリング装置において：コンピュータを、前記コンテンツデータ (Content) を記憶するコンテンツ記憶手段と；前記コンテンツデータ (Content) 毎にユニークに割り当てられるコンテンツ識別子 (CID) と、前記オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、前記コンテンツデータ (Content) を暗号化するコンテンツ鍵 (Kc) および前記コンテンツ鍵をルート鍵 (Root) で暗号化した第2のコンテンツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) と、から成る鍵情報を記憶する鍵情報記憶手段と；前記オーサリング鍵 (CED) から、前記コンテンツ識別子 (CID) と前記オーサリング鍵使用鍵 (CEK) を用いて、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) とを復号化する復号化手段と前記コンテンツ鍵 (Kc) を用いて前記コンテンツデータ (Content) を暗号化して暗号化コンテンツデータ (E (Kc, Content)) を生成する暗号化手段と、して機能させるコンピュータプログラムを記録したコンピュータ読み取り可能な記憶媒体。

【請求項26】 情報配信端末を介して配信するコンテンツデータ (Content) に対して著作権保護の暗号化を施してオーサリングするオーサリング方法であって：前記コンテンツデータ (Content) 毎にユニークに割り当てられるコンテンツ識別子 (CID) と、オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵 (CEK) と、前記コンテンツデータ (Content) を暗号化するコンテンツ鍵 (Kc) および前記コンテンツ鍵をルート鍵 (Root) で暗号化した第2のコンテンツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) とを生成するオーサリング鍵生成段階と；前記オーサリング鍵 (CED) から、前記コンテンツ識別子 (CID) と前記オーサリング鍵使用鍵 (CEK) を用いて、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) とを復号化する復号化段階と；復号化した前記コンテンツ鍵 (Kc) を用いて前記コンテンツデータ (Content) を暗号化し、オーサリングされた暗号化コンテンツデータ (E (Kc, Content)) を生成する暗号化段階と；から成ることを特徴とする、オーサリング方法。

【請求項27】 さらに、前記暗号化装置によって得られる暗号化コンテンツデータ (E (Kc, Content)) と、前記コンテンツ識別子 (CID) と、前記第2のコンテンツ鍵 (EKc) とを一つのパッケージデータとしてパッケージ化するパッケージ段階を含むことを特徴とする、請求項26に記載のオーサリング方法。

【請求項28】 前記ルート鍵 (Root) は、前記コンテンツデータ (Content) を生成可能な再生装置に関連するデバイス鍵 (Kdevice) により暗号化されたコンテンツ使用可能化鍵 (EKB) に組み込まれて保持されており、前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) に加えて前記コンテンツ使用可能化鍵 (EKB) も暗号化されていることを特徴とする、請求項26に記載のオーサリング方法。

【請求項29】 前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) に加えてチェックサム情報も暗号化されていることを特徴とする、請求項26に記載のオーサリング方法。

【請求項30】 前記オーサリング鍵 (CEK) の更新があった場合には、更新前のオーサリング鍵 (CEK) の破棄を行う破棄段階をさらに含むことを特徴とする、請求項26に記載のオーサリング方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、セキュアに楽曲などのコンテンツを配信する情報配信システムに係り、特

50

(5)

特開 2003-69548

7

にメモリスティックなどの記憶媒体にコンテンツをセキュアにダウンロードすることが可能な情報提供装置、情報配信端末、情報提供方法、コンピュータプログラムおよび記憶媒体を介して配信するコンテンツデータに対して、著作権保護の暗号化を施してオーサリングするオーサリングシステム、オーサリング用の鍵を生成するオーサリング鍵生成装置、コンテンツを暗号化してオーサリングするオーサリング装置、オーサリング方法、コンピュータプログラムおよび記憶媒体に関する。

【0002】

【従来の技術】近年、インターネットなどのネットワークの普及とともに、音楽データ、画像（静止画および動画を含む）データ、ゲームプログラムなどの様々な情報（以下、コンテンツという。）をネットワークを介してユーザに対して配信する情報配信システムの構築が提案されている。かかる情報配信システムの構築には、各コンテンツに付随する著作権の保護をどのように担保するかが重要な前提となる。すなわち、ネットワークを介することで、各コンテンツの大量のデジタルコピーが可能となってしまう。そのため、コンテンツの違法コピーを防ぐためのいくつかの著作権保護技術が開発されている。

【0003】

【発明が解決しようとする課題】一般に、配信されるコンテンツを違法コピーから保護するためには、二つの暗号化段階が必要であると言われている。第一の暗号化段階は、コンテンツをオーサリングする際に、コンテンツを暗号化し、コンテンツ配信時の違法コピーを保護する段階である。第二の暗号化段階は、キオスク端末などの情報配信端末を介して、ユーザが所有する記憶装置にコンテンツを書き出す際に、コンテンツを暗号化し、その後の違法コピーを防止する段階である。

【0004】この点、従来のコンテンツ配信サービスにおいては、オーサリング時の暗号化方式と、書き出し時の暗号方式が異なっていた。このため、ユーザが所有する記憶装置にコンテンツを書き出す際に、一旦コンテンツの復号化を行い、再び暗号化するというステップを踏まなければならない、処理に余計な時間を要していた。また、書き出し時の復号化の際に、一時的にコンテンツが生の状態になってしまうためセキュリティ上も問題があった。

【0005】また、従来の情報配信システムにおいては、コンテンツの書き込みモジュールに、使用許可認証機能が備わっていなかったため、書き込みモジュール自体の盗難に対しては無防備であった。すなわち、盗難された書き込みモジュールにより、コンテンツの大量のデジタルコピーを不正に行うことが可能となってしまうという問題もあった。

【0006】さらにまた、従来の情報配信システムにおいては、オーサリング処理自体のプロテクトが甘く、オ

8

ーサリングの仕様書を入力すれば、誰でもコンテンツのオーサリングが可能となってしまうという問題もあった。

【0007】さらにまた、従来の情報配信システムにおいては、例えばコンテンツが音楽データの場合には、ユーザが一旦コンテンツをユーザ所有の記憶装置にダウンロードした後に、他のメディアにコンテンツを移動させたい場合に、正規にコンテンツを入手した正規ユーザであっても、音質を劣化させずに、自由にコンテンツを移動させることはできないという問題もあった。

【0008】さらにまた、従来の情報配信システムにおいては、例えばコンテンツが音楽データである場合には、楽曲とタイトルしかMDなどのメディアに記録できず、ジャケット写真や歌詞データ等の付随データ（いわゆる、フリンジデータ）については、プリンタによりプリントアウトするなどして入手しなければならないという問題もあった。

【0009】本発明は、従来の情報配信システムが有する上記および以下に言及されるような各種問題点を解決することを目的としている。

【0010】

【課題を解決するための手段】上記課題を解決するために、本発明のある観点によれば、情報配信端末を介して配信するコンテンツデータ（Content）に対して著作権保護の暗号化を施してオーサリングするオーサリングシステムが提供される。このオーサリングシステムは、オーサリング鍵生成装置とオーサリング装置とから構成されている。

【0011】オーサリング鍵生成装置は、前記コンテンツデータ（Content）毎にユニークに割り当てられるコンテンツ識別子（CID）と、オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵（CEK）と、前記コンテンツデータ（Content）を暗号化するコンテンツ鍵（Kc）および前記コンテンツ鍵をルート鍵（Root）で暗号化した第2のコンテンツ鍵（EKc）を前記コンテンツ識別子（CID）および前記オーサリング鍵使用鍵（CEK）を用いて暗号化したオーサリング鍵（CED）とを生成する。

【0012】オーサリング装置は、前記オーサリング鍵（CED）から、前記コンテンツ識別子（CID）と前記オーサリング鍵使用鍵（CEK）を用いて、前記コンテンツ鍵（Kc）と前記第2のコンテンツ鍵（EKc）とを復号化する復号化手段と、復号化した前記コンテンツ鍵（Kc）を用いて前記コンテンツデータ（Content）を暗号化し、オーサリングされた暗号化コンテンツデータ（E（Kc，Content））を生成する暗号化手段とを備えている。

【0013】オーサリング装置は、前記暗号化手段によって得られる暗号化コンテンツデータ（E（Kc，Content））と、前記コンテンツ識別子（CID）

50

と、前記第2のコンテンツ鍵(EKc)とを一つのパッケージデータとしてパッケージ化するパッケージ手段をさらに備えてもよい。

【0014】上記課題を解決するために本発明の別の観点によれば、情報配信端末を介して配信するコンテンツデータ(Content)に対して著作権保護の暗号化を施してオーサリングするためのオーサリング鍵を生成するオーサリング鍵生成装置であって：前記コンテンツデータ(Content)毎にユニークに割り当てられるコンテンツ識別子(CID)と、オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵(CEK)と、前記コンテンツデータ(Content)を暗号化するコンテンツ鍵(Kc)および前記コンテンツ鍵をルート鍵(Kroot)で暗号化した第2のコンテンツ鍵(EKc)を前記コンテンツ識別子(CID)および前記オーサリング鍵使用鍵(CEK)を用いて暗号化したオーサリング鍵(CED)とを生成することを特徴とする、オーサリング鍵生成装置が提供される。

【0015】さらに本発明の別の観点によれば、情報配信端末を介して配信するコンテンツデータ(Content)に対して著作権保護の暗号化を施してオーサリングするオーサリング装置において：前記コンテンツデータ(Content)を記憶するコンテンツ記憶手段と；前記コンテンツデータ(Content)毎にユニークに割り当てられるコンテンツ識別子(CID)と、前記オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵(CEK)と、前記コンテンツデータ(Content)を暗号化するコンテンツ鍵(Kc)および前記コンテンツ鍵をルート鍵(Kroot)で暗号化した第2のコンテンツ鍵(EKc)を前記コンテンツ識別子(CID)および前記オーサリング鍵使用鍵(CEK)を用いて暗号化したオーサリング鍵(CED)と、から成る鍵情報を記憶する鍵情報記憶手段と；前記オーサリング鍵(CED)から、前記コンテンツ識別子(CID)と前記オーサリング鍵使用鍵(CEK)を用いて、前記コンテンツ鍵(Kc)と前記第2のコンテンツ鍵(EKc)とを復号化する復号化手段と；前記コンテンツ鍵(Kc)を用いて前記コンテンツデータ(Content)を暗号化して暗号化コンテンツデータ(E(Kc, Content))を生成する暗号化手段とを備えることを特徴とする、オーサリング装置が提供される。

【0016】このオーサリング装置は、さらに、前記暗号化手段によって得られる暗号化コンテンツデータ(E(Kc, Content))と、前記コンテンツ識別子(CID)と、前記第2のコンテンツ鍵(EKc)とを一つのパッケージデータとしてパッケージ化するパッケージ手段を備えてもよい。

【0017】また、前記オーサリング鍵(CED)は、前記パッケージデータ作成装置とは別体に構成された構

限のあるオーサリング鍵生成装置において暗号化されるように構成してもよい。

【0018】さらに、前記パッケージ手段は、さらに前記コンテンツデータ(Content)に関する付加情報であるブリッジデータを合わせてパッケージ化するように構成してもよい。

【0019】さらに本発明の別の観点によれば、コンピュータをして上記オーサリング鍵生成装置または上記オーサリング装置として機能せしめることを特徴とするコンピュータプログラムおよびそのコンピュータプログラムが格納されたコンピュータ読み取り可能な記憶媒体が提供される。

【0020】上記オーサリングシステム、オーサリング鍵生成装置、オーサリング装置において、前記コンテンツ鍵(Kc)は、前記第2のコンテンツ鍵(EKc)と前記ルート鍵(Kroot)から得られる鍵であって、前記暗号化コンテンツデータ(E(Kc, Content))を復号可能とし、前記ルート鍵(Kroot)をセキュアに保持する再生装置において前記コンテンツデータ(Content)を再生可能とするように構成してもよい。

【0021】前記ルート鍵(Kroot)は、前記再生装置に関連するデバイス鍵(Kdevice)により暗号化されたコンテンツ使用可能化鍵(EKB)に組み込まれて保持されており、前記オーサリング鍵(CEK)には、前記コンテンツ鍵(Kc)と前記第2のコンテンツ鍵(EKc)に加えて前記コンテンツ使用可能化鍵(EKB)も暗号化されているように構成してもよい。

【0022】また、前記オーサリング鍵(CEK)には、前記コンテンツ鍵(Kc)と前記第2のコンテンツ鍵(EKc)に加えてチェックサム情報も暗号化するように構成してもよい。

【0023】さらに、前記オーサリング鍵(CEK)の更新があった場合には、更新前のオーサリング鍵(CEK)の破棄を行う破棄手段をさらに備えるように構成してもよい。

【0024】本情報配布システムの情報配布対象である前記コンテンツデータ(Content)は、メインコンテンツデータとメインコンテンツデータの付加情報とを含んでいる。

【0025】さらに本発明の別の観点によれば、情報配信端末を介して配信するコンテンツデータ(Content)に対して著作権保護の暗号化を施してオーサリングするオーサリング方法であって：前記コンテンツデータ(Content)毎にユニークに割り当てられるコンテンツ識別子(CID)と、オーサリング装置毎にユニークに割り当てられるオーサリング鍵使用鍵(CEK)と、前記コンテンツデータ(Content)を暗号化するコンテンツ鍵(Kc)および前記コンテンツ鍵をルート鍵(Kroot)で暗号化した第2のコンテン

(7)

特開 2003-69548

11

12

ツ鍵 (EKc) を前記コンテンツ識別子 (CID) および前記オーサリング鍵使用鍵 (CEK) を用いて暗号化したオーサリング鍵 (CED) とを生成するオーサリング鍵生成段階と; 前記オーサリング鍵 (CED) から、前記コンテンツ識別子 (CID) と前記オーサリング鍵使用鍵 (CEK) を用いて、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) とを復号化する復号化段階と; 復号化した前記コンテンツ鍵 (Kc) を用いて前記コンテンツデータ (Content) を暗号化し、オーサリングされた暗号化コンテンツデータ (E (Kc, Content)) を生成する暗号化段階と; から成ることを特徴とする、オーサリング方法が提供される。

【0026】上記オーサリング方法は、さらに、前記暗号化装置によって得られる暗号化コンテンツデータ (E (Kc, Content)) と、前記コンテンツ識別子 (CID) と、前記第2のコンテンツ鍵 (EKc) とを一つのパッケージデータとしてパッケージ化するパッケージ段階を含んでもよい。

【0027】前記ルート鍵 (Kroot) は、前記コンテンツデータ (Content) を生成可能な再生装置に関連するデバイス鍵 (Kdevice) により暗号化されたコンテンツ使用可能化鍵 (EKB) に組み込まれて保持されており、前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) に加えて前記コンテンツ使用可能化鍵 (EKB) も暗号化されているように構成しても良い。

【0028】前記オーサリング鍵 (CEK) には、前記コンテンツ鍵 (Kc) と前記第2のコンテンツ鍵 (EKc) に加えてチェックサム情報も暗号化されているように構成してもよい。

【0029】前記オーサリング鍵 (CEK) の更新があった場合には、更新前のオーサリング鍵 (CEK) の破棄を行う破棄段階をさらに含むように構成しても良い。

【0030】本発明のさらに別の目的、特徴、作用効果については、以下に述べる発明の実施形態および添付図面により明らかになろう。

【0031】

【発明の実施形態】以下に添付図面を参照しながら、本発明にかかる情報配信システム等の好適な実施形態として、当該システムを音楽データをコンテンツとして配信する情報配信システムに適用した場合について説明する。なお、以下の説明および添付図面において、略同一の機能構成を有する部材については、同一の符号を付することにより重複説明を省略することにする。

【0032】(1. 配信対象となる情報) まず、本実施の形態にかかる情報配信システムの理解を容易にするために、情報配信システムの配信対象となる情報について説明する。

【0033】本実施の形態にかかる情報配信システムに

おける配信対象となる情報は、「配信用コンテンツ」である。配信用コンテンツは、メインコンテンツと付加情報を含んでいる。なお、本明細書において、単に「コンテンツ (データ)」と称した場合には、後述するメインコンテンツと付加情報の双方を含むものとする。

【0034】「メインコンテンツ (データ) (Main Content Data)」は、本実施の形態にかかる情報配信システムにおける主たる配信対象となる情報である。より具体的には、コンテンツホルダにより制作される楽曲データ、画像データ (静止画像データおよび動画データを含む)、ゲームプログラムなどである。

【0035】「付加情報」は、メインコンテンツに付随するデータである。例えば、メインデータが楽曲データである場合には、それに付随したジャケット写真や歌詞などといったフリンジデータ (Fringe Data) や、楽曲のタイトルやアーティスト名などのメタデータ (Metadata) や、他の装置へのチェックアウト (Check Out) 可能回数やコンピュータ装置への移動 (Import) 可能回数などの利用条件情報などを含んでいる。

【0036】「パッケージ (データ) (パッケージ情報 (Package Data))」は、本実施の形態にかかる情報配信システムにおいて、情報配信端末から配信する配信用コンテンツデータに対して、著作権保護の暗号化を施してパッケージ化したものである。パッケージデータは、オーサリングスタジオ800のパッケージ情報生成部310により生成される。パッケージには、メインコンテンツおよび付加情報を暗号化した暗号化コンテンツデータ (E (Kc, Content)) に加えて、後述する第2のコンテンツ鍵 (EKc) およびコンテンツ使用可能化鍵 (EKB) など含まれている。

【0037】(2. 情報配信システムの概要) 図1に、本実施の形態にかかる情報配信システム100の概略構成を示す。図1に示すように、情報配信システム100は、コンテンツホルダ部120と、コンテンツ流通部140と、鍵管理装置160と、ユーザ部180とから主に構成されている。以下、各構成要素について説明する。

【0038】(2.1 コンテンツホルダ (Content Holder) 部120) コンテンツホルダ部120は、レコード会社に所属するサーバのような情報処理装置群である。コンテンツホルダ部は同様の機能を有する複数のコンテンツホルダ120a~120nから構成されている。各コンテンツホルダ120a~120nは、例えば、図2に示すように、コンテンツ管理部122と、コンテンツ作成部124と、コンテンツ出力部126と、コンテンツデータベース128とを備えたコンピュータなどのサーバ装置である。

【0039】(コンテンツ管理部122) コンテンツ管

10

20

30

40

50



(8)

特開2003-89548

13

14

理部122は、当該コンテンツホルダ120aに関連するレコード会社などにより制作された楽曲データなどのコンテンツを管理する。ここで管理されるコンテンツには、コンテンツが音楽関連情報の場合には、楽曲データなどのメインコンテンツに加え、ジャケット写真や歌詞データなどのフリジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【0040】(コンテンツ作成部124) コンテンツ作成部124は、当該コンテンツホルダ120aに関連するコンテンツを作成する。ここで作成されるコンテンツには、コンテンツが音楽関連情報の場合には、楽曲データなどのメインコンテンツに加え、ジャケット写真や歌詞データなどのフリジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【0041】(コンテンツ出力部126) コンテンツ出力部126は、当該コンテンツホルダ120aにおいて作成管理されるコンテンツを、後述するようなコンテンツ流通部140のコンテンツアグリゲータ200に受け渡す。コンテンツの受け渡しは、インターネットなどのネットワークを介して行ってもよいし、あるいは、CD-RやDVD-RAMなどの記憶メディアを介して行ってもよい。

【0042】(コンテンツデータベース128) コンテンツデータベース128は、コンテンツ作成部124により作成されたコンテンツを記憶する大容量記憶メディアである。ここで記憶され管理されるコンテンツには、コンテンツが音楽関連情報の場合には、楽曲データなどのメインコンテンツに加え、ジャケット写真や歌詞データなどのフリジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【0043】(2.2 コンテンツ流通部) コンテンツ流通部140は、本実施の形態にかかる情報配信システムの中核をなす部分である。このコンテンツ流通部140において、配信用コンテンツに対して著作権保護のための暗号化が施され、パッケージデータとしてパッケージ化される。パッケージ化されたパッケージデータは、ネットワーク600を介してキオスク端末などの情報配信端末400に送られ、情報配信端末400からユーザが所有する記憶装置182に提供される。

【0044】コンテンツ流通部140は、コンテンツアグリゲータ部200と、オーサリングスタジオ部300と、情報配信部(キオスク端末部)400と、認証サーバ部500と、ネットワーク600とから主に構成されている。

【0045】(2.2.1 コンテンツアグリゲータ(Content Aggregator)200) コンテンツアグリゲータ200は、コンテンツホルダ12

0から楽曲などのコンテンツを収集し、企画編成する業務を行う。ここで収集されるコンテンツには、コンテンツが音楽関連情報の場合には、楽曲データなどのメインコンテンツに加え、ジャケット写真や歌詞データなどのフリジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【0046】コンテンツアグリゲータ200は、コンテンツ管理部210と、コンテンツ収集部220と、コンテンツ出力部230と、コンテンツデータベース240とから主に構成されている。

【0047】(コンテンツ管理部210) コンテンツ管理部210は、コンテンツホルダ120a~120nが保持しているコンテンツの中から、情報配信システム100を利用して配信を行う魅力と価値のあるコンテンツを選択する。さらにコンテンツ管理部210は、コンテンツ収集部220に対して、所定のコンテンツホルダ120aに直接アクセスして、あるいは所定のコンテンツホルダ120aから配布されるメディアにアクセスして、コンテンツを収集するように指令を行う。コンテンツ管理部210は、コンテンツホルダ120から収集したコンテンツの企画編成も同時に行う。

【0048】(コンテンツ収集部220) コンテンツ収集部220は、コンテンツ管理部210からの指令を受けて、所定のコンテンツホルダ120aに直接アクセスして、あるいは所定のコンテンツホルダ120aから配布されるメディアにアクセスして、コンテンツを取り込み、コンテンツデータベース240に記憶する。

【0049】(コンテンツデータベース240) コンテンツデータベース240は、コンテンツ収集部220が取り込んだコンテンツを一時的に記憶して管理する。またコンテンツデータベース240は、コンテンツアグリゲータ200の動作に関する各種履歴を記憶して管理する。

【0050】(コンテンツ出力部230) コンテンツ出力部230は、後述するオーサリングスタジオ300からの要求に応じて、コンテンツ収集部220が収集したコンテンツをコンテンツデータベース240から読み出し、オーサリングスタジオ300に対して出力する。オーサリングスタジオ300へのコンテンツの出力は、インターネットなどの公衆回線網を介して行ってもよいし、よりセキュアな専用回線網を介しておこなってもよい。さらには、CD-RやDVD-RAMなどの記憶媒体を介して行ってもよい。

【0051】(2.2.2 オーサリングスタジオ300) オーサリングスタジオ300は、配布対象であるコンテンツを本実施の形態にかかる情報配信システムに適合するように加工する機能を有する。より具体的に言えば、コンテンツデータの加工は、コンテンツを配布しやすいように圧縮する第一段階と、オーサリングして暗号

(9)

特開2003-69548

15

16

化し、さらにパッケージ化する第二段階を経て行われる。

【0052】図4に示すように、オーサリングスタジオ300は、オーサリング部310と商品管理部330とデータベースサーバ340とから主に構成されている。

【0053】(オーサリング部310) オーサリング部310は、例えばコンピュータ装置上で動作するコンピュータプログラムであり、図5に示すように、コンテンツ管理部312と、データ圧縮部314と、パッケージ生成モジュール316と、GUI制作部318と、配信部320とを備えている。

【0054】(コンテンツ管理部312) コンテンツ管理部312は、コンテンツアグリゲータ200から受信したコンテンツを管理する。ここで管理されるコンテンツには、コンテンツが音楽関連情報の場合には、楽曲データなどのメインコンテンツに加え、ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報が含まれている。

【0055】(データ圧縮部312) データ圧縮部312は、例えば、コンテンツ管理部312から受け渡されたコンテンツを圧縮加工するソフトウェアである。圧縮方式としては、例えばコンテンツが楽曲データであるような場合には、ATRAC3方式を採用して、元データを約1/10に圧縮加工することが可能である。もちろん、圧縮方式は、ATRAC3 (Adaptive Transform Acoustic Coding 3) に限定されず、MP3 (MPEG-1 Audio Layer 3) 方式、AAC (Advanced Audio Coding) 方式、WMA (Windows (登録商標) Media Audio) 方式、Twins VQ (Transform-Domain Weighted Interleave Vector Quantization) 方式、QDX方式などの音声圧縮方式を採用することが可能であることはいうまでもない。

【0056】(パッケージ生成部(オーサリング装置)316) パッケージ生成部(オーサリング装置)316は、例えば、データ圧縮部314において圧縮加工されたコンテンツデータをオーサリングするために暗号化するとともにパッケージ化する機能を有するソフトウェアとして構成される。すなわち、パッケージ生成部316は、コンテンツデータをオーサリングするオーサリング装置として機能する。

【0057】オーサリング装置316の構成およびオーサリング装置で用いられるいくつかの鍵の詳細については、オーサリング鍵生成装置160と関連して後述することとし、ここでは簡単な説明にとどめる。

【0058】オーサリング装置316は、図6に示すように、コンテンツ鍵(Kc)復号化手段3162と、コ

ンテンツ暗号化手段3164と、パッケージ手段3166とから主に構成されている。

【0059】(コンテンツ鍵(Kc)復号化手段3162) コンテンツ鍵(Kc)復号化手段3162は、後述するオーサリング鍵生成装置160から、オーサリング鍵(CED)と前記コンテンツ識別子(CID)と前記オーサリング鍵使用鍵(CEK)とを受け取る。そして、オーサリング鍵(CED)から、コンテンツ識別子(CID)とオーサリング鍵使用鍵(CEK)を用いて、コンテンツ鍵(Kc)と第2のコンテンツ鍵(EKc)とを復号化する。

【0060】(コンテンツ暗号化手段3164) コンテンツ暗号化手段3164は、コンテンツ鍵(Kc)復号化手段3162により復号化した前記コンテンツ鍵(Kc)を用いて、コンテンツデータを暗号化し、暗号化コンテンツデータ(E(Kc, Content))を生成する。本実施の形態にかかる情報配信システムでは、この暗号化コンテンツデータ(E(Kc, Content))が所定の情報とともにパッケージ化されて情報配信端末400に送信される。

【0061】(パッケージ手段3166) パッケージ手段3166は、コンテンツ暗号化手段3164によって得られる暗号化コンテンツデータ(E(Kc, Content))と、コンテンツ識別子(CID)と、第2のコンテンツ鍵(EKc)とを一つのパッケージデータとしてパッケージ化する。パッケージには、楽曲データなどのメインコンテンツに加え、ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利用条件情報などの付加情報も含まれる。

【0062】(パッケージ生成部316の機能構成図) 図7には、パッケージ生成部316の機能をより具体的に示すブロック図が示されている。図示のように、パッケージ生成部316は、Windows 2000のようなOS 310a上で動作するオーサリングアプリケーション310bとして構成されている。オーサリングアプリケーション310b内には、データ圧縮部314とパッケージ生成部316などがDLL (Dynamic Link Library) として、組み込まれている。なお、オーサリングアプリケーション310bに組み込まれるコンテンツ管理部312などの他のアプリケーションは説明の便宜のため図示を省略している。

【0063】図示のように、所定の音声形式、例えばWAV形式で構成された圧縮前の楽曲データがデータ圧縮部314に送られ、所定の圧縮形式、例えばATRAC3形式で圧縮される。データ圧縮部314において圧縮された楽曲データなどのメインコンテンツは、パッケージ生成部316に送られ、フリンジデータやメタデータや利用条件情報などから構成される付加情報とともに、暗号化され、パッケージ化される。

【0064】このように、本実施の形態にかかるオーサリング装置（パッケージ生成装置）316によれば、オーサリング時に、データ圧縮、暗号化、パッケージ化といった処理を行ってしまうことが可能である。その結果、コンテンツの流通時やコンテンツの販売時における演算付加や通信負荷を軽減することができる。特に情報配布端末におけるダウンロード時間が大幅に縮小可能であり、ユーザは、コンテンツのコピー時間とほとんど変わらない時間でオーサリングされたコンテンツのダウンロードを行うことができる。

【0065】（GUI制作部318）再び図5を参照して、オーサリング部310のGUI制作部318は、後述する情報配信端末であるキオスク端末に表示されるGUI（Graphical User Interface）を制作する機能を有する。ここで制作されたGUIは、配信部320を介して、各キオスク端末に配布される。コンテンツをダウンロードしたいユーザは、このGUIに基づいてキオスク端末上に表示される画面にナビゲートされながら、コンテンツを購入し、所定の記憶媒体にダウンロードしたり、あるいはダウンロードしたコンテンツをコンピュータ装置などの移動（Import）したり、そのコンピュータ装置などから他の再生装置や記憶媒体にチェックアウトしたりすることが可能である。

【0066】（配信部320）配信部320は、上記のようにデータ圧縮部314およびパッケージ生成部316を含むパッケージアプリケーションにより圧縮され、パッケージ化されたコンテンツや、GUI制作部318において制作されたGUIを、キオスク端末などの情報配信端末400に配信する機能を有している。

【0067】（商品管理部330）再び図4を参照して、商品管理部330は、オーサリング部310において、配信用に加工されたコンテンツをパッケージ商品として管理する。具体的には、商品管理部330は、パッケージ化されたコンテンツの流通を監視し、キオスク管理センタの販売管理部などと連携して、商品の販売および代金回収業務を行う。また商品管理部330は、情報配信端末であるキオスク端末400における販売履歴などについても統計的に把握して管理し、将来的な商品開発の資料とする。商品管理部330の業務履歴は、データベースサーバ340に記憶される。

【0068】（データベースサーバ340）データベースサーバ340は、オーサリングスタジオ300に関連する各種データを記憶して管理する。具体的には、データベースサーバ340は、オーサリング310において、配信用に加工されたコンテンツを記憶する。ここで管理されるコンテンツには、コンテンツが音楽関連情報の場合には、楽曲データなどのメインコンテンツに加え、ジャケット写真や歌詞データなどのフリンジデータや楽曲タイトルやアーティスト名などのメタデータや利

用条件情報などの付加情報が含まれている。

【0069】また、データベースサーバ340には、商品管理部330の業務履歴、すなわち、パッケージ商品の販売情報や代金回収情報、情報配信端末であるキオスク端末における販売履歴などについて記憶して管理する。

【0070】（2. 2. 3 情報配信端末400）情報配信端末400は、キオスク端末とも称されるものであり、オーサリングスタジオ300から配信されたパッケージ化されたコンテンツを記憶し、ユーザ180からの要求に応じて該当するコンテンツをユーザ180の記憶媒体182にダウンロードする機能を有する。キオスク端末400は、コンビニエンスストアやガソリンスタンドなどの人が集まりやすい場所に設置しても構わないし、各個人が利用する場所に設置されるパーソナルコンピュータ装置を情報配信端末としても構わない。

【0071】情報配信端末400は、図8に記載されているように、情報配信端末管理部410、情報提供部420、リーダ/ライタ（R/W）430、販売管理部440、課金制御部450、データベース460から主に構成されている。

【0072】（情報配信端末管理部410）情報配信端末管理部410は、例えば、情報配信端末400におけるさまざまな業務を管理するソフトウェアである。情報配信端末管理部410は、情報提供部420およびリーダ/ライタ（R/W）430と連携して、情報配信端末装置の外部認証および内部認証を管理するとともに、認証終了後には、リーダ/ライタ（R/W）430を介してメモリスティックなどの記憶装置182へのコンテンツの書き込みを許可する。

【0073】情報配信端末管理部410は、販売管理部440および課金制御部450と連携して、ユーザ部180に対するコンテンツの販売業務および課金業務を管理する機能も有する。情報配信管理部410は、さらに、パッケージ化されたコンテンツを格納したり、あるいは販売業務や課金業務に関する履歴を格納するデータベース460を管理している。

【0074】（情報提供部420）情報提供部420は、パッケージが正規のオーサリングシステムにより作成されたものかどうかなどの検証動作や認証動作を行い、認証が肯定的である場合に、コンテンツをリーダ/ライタ（R/W）430を介してメモリスティックなどの記憶装置182への書き込みを行う機能を有している。

【0075】情報提供部420は、図9に示すように、外部認証部422と、内部認証部424と、再生制御部428とから主に成るソフトウェアとして構成することができる。

【0076】情報提供部420は、例えば、情報配布端末400に組み込まれたDLL（Dynamic Li

nk Library)として構成される。情報提供部420を、所定のOS、例えばWindows 2000上で動作するアプリケーションとして組み込んだ一例を図12に示す。なお、図12に示す情報提供部420は、理解を容易にするために、GUIアプリケーション部423と、セキュアモジュール部425と、インタフェース部427とから構成している。

【0077】(外部認証部422)再び図9を参照して、外部認証部422は、情報提供部420が正規のものであるか、すなわち情報配布端末400が記憶しているコンテンツを外部に提供する権限を有するかどうかを、情報提供部420が予め保管する第1の外部認証鍵(Kauth(1))と、認証サーバ500が保管する第2の外部認証鍵(Kauth(2))とを用いて、比較認証する機能を有している。

【0078】外部認証は、情報提供部420を起動するたびに必ず行う必要がある。ただし、一度認証が通れば、情報提供部420の起動中は再度行わなくてもよい。

【0079】外部認証部422は、図10に示すように、外部認証管理部4221と、鍵保持手段4222と、乱数発生手段4223と、第1の暗号化手段4224と、第2の暗号化手段4225と、比較手段4226と、送受信手段4227とから主に構成されている。

【0080】(外部認証管理部4221)外部認証管理部4221は、外部認証部422における認証動作を全体的に管理する。外部認証管理部4221は、情報提供部420が起動されると、後述する外部認証を行い、外部認証が成功すると、内部認証部424に処理を受け渡すように動作する。

【0081】(鍵保持手段4222)鍵保持手段4222は、第1の外部認証鍵(Kauth(1))をセキュアに保持する。第1の外部認証鍵(Kauth(1))は、認証サーバ部500から事前に、情報提供部420に配布されるが、この第1の外部認証鍵(Kauth(1))は、情報提供部420の認証部(セキュアモジュール)内にタンパレジスタント(Tamper Resistant)に隠蔽されているので、リバースエンジニアリングしても値を調べるのが困難である。

【0082】(乱数発生手段4223)乱数発生手段4223は、外部認証用の乱数を発生する。乱数発生手段4223で発生された乱数は、一方で、第1の暗号化手段4224に送られ第1の外部認証鍵(Kauth(1))により暗号化され第1の暗号化データを生成する。他方で、乱数発生手段4223で発生された乱数は、第2の暗号化手段4225に送られ第2の外部認証鍵(Kauth(2))により暗号化され第2の暗号化データを生成する。

【0083】(第1の暗号化手段4224)第1の暗号化手段4224は、基本的には、情報提供部420内に

組み込まれているソフトウェアである。第1の暗号化手段4224は、乱数発生手段4223が発生した乱数を、鍵保持手段4222にセキュアに保持された第1の外部認証鍵(Kauth(1))を用いて暗号化し第1の暗号化データを生成する。

【0084】(第2の暗号化手段4225)第2の暗号化手段4225は、乱数発生手段4223が発生した乱数を、第1の暗号化手段4224とは別のルートで、第1の外部認証鍵(Kauth(1))と同一の第2の外部認証鍵(Kauth(2))を用いて暗号化して第2の暗号化データを取得する。

【0085】第2の暗号化手段4225による第2の暗号化データ取得の構成は、要求されるセキュリティレベルに応じて、さまざまな実施形態を採用可能である。

【0086】(ローカル外部認証)最もセキュリティレベルが低い実施形態は、図13に示すように、ローカルで、すなわち情報提供部420内において外部認証を行う。この実施形態においては、第2の暗号化手段4225も情報提供部420内に組み込まれ、情報提供部420内に事前に組み込まれた第2の外部認証鍵(Kauth(2))を用いて乱数を暗号化して第2の暗号化データを取得する。

【0087】しかしながら、かかるローカルな外部認証の態様では、情報配布端末400を悪意に操作する者に第2の外部認証鍵(Kauth(2))が盗まれる可能性がある。また情報配布端末400自体を盗まれた場合には、情報配布端末400内に記憶されたパッケージのダウンロードが可能になってしまう。したがって、上記のようなローカルな外部認証は、情報配布端末自体を盗まれないように設計してある場合や、盗まれるとデータが破壊されるように設計している場合には有効である。なお、図18に示す実施形態における外部認証動作については後述する。

【0088】(リモート外部認証)これに対して、最もセキュリティレベルの高い実施形態は、図14に示すように、リモートで、すなわち情報提供部420の外部にある認証サーバ500を利用して外部認証を行う。この実施形態においては、認証サーバ部500は、認証サーバ部500内に上記乱数を取り込んで、第2の外部認証鍵(Kauth(2))を用いて第2の暗号化データを生成する。

【0089】したがって、第2の外部認証鍵(Kauth(2))が盗まれることがなく、また情報配布端末400自体を盗まれた場合であっても、情報配布端末400内に記憶されたパッケージのダウンロードを行うことはできない。なお、図14に示す実施形態における外部認証動作については後述する。

【0090】(セミローカル外部認証)さらに、図13に示す実施形態と図14に示す実施形態との中位のセキュリティレベルを有する実施形態を図15に示す。この

(12)

特開 2003-69548

21

実施形態においては、認証サーバ部500は、必要に応じて、例えばダウンロードを行う際に、第2の外部認証鍵(Kauth(2))を情報提供部420に一時的に受け渡される。情報提供部420は認証サーバ部500から受け渡された第2の外部認証鍵(Kauth(2))を用いて乱数を暗号化し、第2の暗号化データを生成する。第2の暗号化データが生成された後に、あるいは情報配布端末400への電源が遮断されることに、第2の外部認証鍵(Kauth(2))は情報提供部420から消去される。

【0091】この実施形態によれば、ダウンロードなどの必要な時にのみ、第2の外部認証鍵(Kauth(2))が情報配布端末400に一時的に受け渡されるので、第2の外部認証鍵(Kauth(2))自体の盗難による被害のおそれが著しく軽減される。また情報配布端末400自体を盗まれた場合であっても、第2の外部認証鍵(Kauth(2))を、情報配布端末400の電源が遮断された時点で消去されるように構成すれば、情報配布端末400内に記憶されたパッケージのダウンロードを行うことはできない。なお、図15に示す実施形態における外部認証動作については後述する。

【0092】(比較手段4226)比較手段4226は、第1の暗号化手段4224が生成した第1の暗号化データと第2の暗号化手段4225が生成した第2の暗号化データとを比較する。比較の結果、第1の暗号化データと第2の暗号化データとが一致する場合に、外部認証が完了する。

【0093】(送受信手段4227)送受信手段4227は、外部認証部422における情報の送受信を行う。送受信手段4227は、例えば、乱数発生手段4223が発生した乱数を外部に送信したり、認証サーバ500などから第2の暗号化手段4225が取得した第2の暗号化データを取り込んだりする。

【0094】(内部認証部424)内部認証部424は、情報提供部420の外部認証完了後に行われる内部認証を行う機能を有する。内部認証部424は、図11に示すように、第1の認証手段4242と、第2の認証手段4244とから構成されている。

【0095】(第1の認証手段4242)第1の認証手段4242は、配布対象であるコンテンツデータが、正規のオーサリングシステム(オーサリングスタジオ300)により作成されたコンテンツであるかを認証するための手段を提供する。具体的には、第1の認証は、正規のオーサリングシステムが前記コンテンツデータに書き込んだMAC(Message Authentication Code)値を検証して行われる。

【0096】MAC値は、メインコンテンツに付随する付随データのうち利用条件情報をコンテンツ鍵(Kc)を用いて計算される。そのため、MAC値は、コンテンツ鍵(Kc)およびルート鍵(Kroot)を知らない

22

と計算することができないため、情報提供部420とオーサリング鍵(CED)を供給された者でないとパッケージデータを作成できない。

【0097】(第2の認証手段4244)第2の認証手段4244は、記録手段であるリーダ/ライタ430と情報記録管理手段である情報提供装置420との相互認証を行うための手段を提供する。第2の認証手段4244は、まず、正規のオーサリングシステム300がルート鍵(Kroot)をデバイス鍵(Kdevice)で暗号化したコンテンツ使用可能化鍵(EKB)を、リーダ/ライタ430と情報提供装置420との双方に受け渡す。リーダ/ライタ430と情報提供装置420は、それぞれがセキュアに保持するデバイス鍵(Kdevice)を用いてルート鍵(Kroot)を復号化させる。そして、復号化されたルート鍵(Kroot)が相互に一致する場合に肯定的な認証を行う。

【0098】(再生制御部428)再生制御部428は、内部認証の結果、ルート鍵(Kroot)の共有が認証されたメモリスティックなどの所定の記憶媒体においてコンテンツデータを再生可能とするものである。再生制御部428は、リーダ/ライタ430が記憶媒体に複数のコンテンツデータを一括して記録する場合には、複数のコンテンツ全ての記録が終了した後に、複数のコンテンツの再生を可能とするように構成されている。

【0099】(リーダ/ライタ(R/W)430)リーダ/ライタ(R/W)430は、メモリスティック、メモ리카ード、スマートメディアなどの記憶媒体に、コンテンツをダウンロードするためのハードウェアである。すでに説明したように、ダウンロードを行う前に、情報提供部420とリーダ/ライタ(R/W)430間において、内部認証を行い、相互に正規の装置であることを確認した上で、ダウンロードを行う。

【0100】(販売管理部440)販売管理部440は、パッケージ化されたコンテンツの販売時に生じる様々な業務を管理する。販売管理部440は、さらに、販売履歴を管理して、販売情報を収集する。販売管理部440は、例えば、どの時間帯に、どのような年齢層の男性または女性に、どの程度の値段の、どのようなジャンルのコンテンツが、どの程度の数量販売されたかなどについての統計的情報を収集し、将来的な商品開発に役立てることができる。

【0101】(課金制御部450)課金制御部450は、パッケージ化されたコンテンツの販売時に生じる課金ベースの業務を管理する。課金制御部450は、例えばユーザが現金で支払を行う場合には、つり銭などの精算業務を管理する。課金制御部450は、例えばユーザがクレジットカードなどで支払を行う場合には、本人照会や信用照会などの業務を管理する。

【0102】データベース460は、情報配信端末400に関連する各種情報を格納し管理する。データベース

(13)

特開 2009-69548

23

460には、例えば、本実施の形態にかかる情報配布システム100の配布対象であるパッケージ化されたコンテンツや、販売履歴や課金履歴などの各種履歴情報などが格納されている。

【0103】(2. 2. 4 認証サーバ部500) 認証サーバ部500は、ある情報配信端末400がコンテンツのダウンロードを行う権限を有する正規の情報配信端末であるか外部認証を行う機能を有している。本実施の形態にかかる情報配信システム100においては、情報配信端末400は、所定のパッケージ化されたコンテンツをダウンロードする前に、所定の記憶媒体にダウンロード許可権限を有する情報提供部420が正規の装置であるか否かを外部認証する必要がある。

【0104】認証サーバ部500は、情報提供部420の外部認証を行う機能を有している。外部認証は、後述するように、一方で、情報提供部420内において、乱数発生手段423により発生された乱数を鍵保持手段422内にセキュアに保持された第1の外部認証鍵(Kauth(1))を用いて暗号化し、第1の暗号化データを生成する。第1の外部認証鍵(Kauth(1))は、認証サーバ部500から事前に、情報提供部420に配布されるが、この第1の外部認証鍵(Kauth(1))は、情報提供部420の認証部(セキュアモジュール)内にタンパレジスタント(Tamper Resistant)に隠蔽されているので、リバースエンジニアリングしても値を調べることは困難である。

【0105】他方、別のルートで、第1の外部認証鍵(Kauth(1))と同一の第2の外部認証鍵(Kauth(2))を用いて同様の乱数を暗号化して第2の暗号化データを取得する。そして、情報提供部420内において発生された第1の暗号化データと、第1の暗号化データとは別ルートで生成された第2の暗号化データとを比較し、両者が一致した場合に、情報提供部420が正規のものであると外部認証するように構成されている。

【0106】認証サーバ部500は、基本的には、上記外部認証工程において、第2の外部認証鍵(Kauth(2))を管理している。後述するように、ある実施形態においては、認証サーバ部500は、認証サーバ部500内に上記乱数を取り込んで第2の外部認証鍵(Kauth(2))を用いて第2の暗号化データを生成する。別の実施形態においては、認証サーバ部500は、第2の外部認証鍵(Kauth(2))を情報提供部420に受け渡して第2の暗号化データを生成する。なお、第2の外部認証鍵(Kauth(2))を情報提供部420内にセキュアに保持する別の実施形態においては、認証サーバ部500が事前に第2の外部認証鍵(Kauth(2))に配布する。

【0107】なお、認証サーバ部500が管理する第1および第2の外部認証鍵(Kauth(1))(2)の

24

発行および管理に関しては、権限のある鍵管理装置160に委託することが可能である。鍵管理装置160は、第1および第2の外部認証鍵(Kauth(1))

(2)を発行するのみならず、例えば、情報配信端末400が盗難にあったような場合には、第1および第2の外部認証鍵(Kauth(1))(2)の内容を更新し、盗まれた情報配信端末400の情報提供部420を無効化することが可能である。

【0108】(2. 2. 5 ネットワーク部600) ネットワーク部600は、オーサリングスタジオ300においてパッケージ化されたコンテンツを情報配信端末400に配信する通信網である。ネットワーク部600は、衛星通信網のような無線通信網600aと、専用回線網600bの双方を含んでいる。セキュリティを確保するためには、ネットワーク部600は、閉鎖系である専用回線網600bから構成することが好ましいが、もちろん、インターネットなどの開放系のネットワークとして構成しても構わない。また、多数の情報配信端末400に同時に配信を行うのであれば、衛星通信網のような無線通信網600aの利用が好適である。

【0109】(2. 3 鍵管理装置) 鍵管理装置160は、本実施の形態にかかる情報配信システムの各段階において利用される鍵を管理する権限のある管理者である。鍵管理装置160は、オーサリング装置316に対してはオーサリング鍵生成装置として機能する。ここで管理される鍵および鍵関連情報は以下の通りである。また、鍵情報は、定期的にまたは必要に応じて更新され、環境変化に対応するとともに、セキュリティの向上が図られる。

【0110】(2. 3. 1 オーサリングスタジオ300において使用される鍵情報) 「コンテンツ鍵(Kc)」は、オーサリングスタジオ300において、コンテンツを暗号化する際に使用される鍵である。コンテンツ鍵(Kc)はルート鍵(Kroot)により暗号化され、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)に加工される。

【0111】「コンテンツ識別子(CID)」は、コンテンツ毎に割り振られる識別子である。コンテンツID(CID)は、各コンテンツに固有の識別子であり、重複して設定されることはない。コンテンツ識別子(CID)の生成は、オーサリング作業の現場ではなく、オーサリング鍵生成装置160において管理するので、コンテンツ識別子(CID)のユニーク性を完全に保証することができる。

【0112】「ルート鍵(Kroot)」は、コンテンツ鍵(Kc)を暗号化する際に使用される鍵である。ルート鍵(Kroot)は、「コンテンツ鍵暗号化鍵」とも称されることがある。共通に使用されるルート鍵(Kroot)は非常に重要な鍵であるが、本システムによれば、このルート鍵(Kroot)をオーサリング装置

316に直接渡すことなく、コンテンツ鍵(Kc)、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)のセットをオーサリング鍵(CED)としてオーサリング装置316に渡すことにより、セキュリティを向上させるとともに、組み合わせの間違いを防止することができる。

【0113】「ルート鍵で暗号化した第2のコンテンツ鍵(EKc)」は、コンテンツ鍵(Kc)をルート鍵(Kroot)で暗号化したものである。EKc=E(Kroot, Kc)と表現できる。コンテンツ鍵(Kc)とルート鍵で暗号化した第2のコンテンツ鍵(EKc)とをセットにしてオーサリング鍵(CED)として生成することにより、組み合わせの間違いを回避できる。

【0114】「デバイス鍵(Kdevice)」は、パッケージ化されたコンテンツを利用可能な再生装置に関する鍵情報である。デバイス鍵は、各再生装置がハードウェア的にあるいはタンパレジスタントソフトにより、セキュアに保持している鍵情報である。

【0115】「コンテンツ使用可能化鍵(EKB: Enabling Key Block)」は、ルート鍵(Kroot)をデバイス鍵(Kdevice)で暗号化したものである。コンテンツ使用可能化鍵(EKB)には、E(KdeviceA, Kroot), E(KdeviceB, Kroot)といったデータが格納されており、再生装置A(DeviceA)は、E(KdeviceA, Kroot)を解くことによりKrootを知ることが可能である。同様に、再生装置B(DeviceB)は、E(KdeviceB, Kroot)を解くことによりKrootを知ることが可能である。

【0116】「オーサリング鍵使用鍵(CEK(Content Enabling Key))」は、コンテンツをオーサリングする事業者と管理者との間で共有される共有秘密情報(鍵)である。オーサリングする事業者毎に異なり、管理者によって発行され管理される。オーサリングする際に、オーサリング鍵(CED)と共に用いられる。

【0117】「オーサリング鍵(CED(Content Enabling Data))」は、コンテンツをオーサリングする時に使用される鍵である。権限のある管理者によって発行され管理される。コンテンツID(CID)と関連付けされており、一つのコンテンツに一つのオーサリング鍵(CED)を用いてオーサリングを行う。オーサリング鍵は、コンテンツ鍵(Kc)およびルート鍵で暗号化した第2のコンテンツ鍵(EKc)をコンテンツID(CID)とオーサリング鍵使用鍵(CEK)で暗号化したものである。

【0118】「冗長コンテンツ鍵ブロック(RKcB(Redundant Kc Block))」は、オーサリング鍵(CED)の中に含まれるべき、コンテン

ツ鍵(Kc)、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)、コンテンツ使用可能化鍵のバージョン情報(EKB-Version)を連結し、さらに不正な解読を困難とするために冗長な乱数情報を付加したデータブロックである。オーサリング鍵(CED)を生成する際に、その生成過程で生成する。オーサリング鍵(CED)を生成する処理過程で使用するデータで、ユーザやアプリケーション開発者には意図されない。

【0119】「チェックサム付冗長コンテンツ鍵ブロック(CRKcB)」は、冗長コンテンツ鍵ブロック(RKcB)のチェックサム(CS)を計算し、冗長コンテンツ鍵ブロック(RKcB)に連結して得られるデータブロックである。

【0120】「最終暗号化鍵(Kcid)」は、オーサリング鍵(CED)作成フローにおいて、最後の暗号化に使用する鍵データである。コンテンツID(CID)とオーサリング鍵使用鍵(CEK)から生成される。最終暗号化鍵(Kcid)自体は、オーサリング鍵(CED)を生成する処理過程で使用するデータであるので、ユーザやアプリケーション開発者には意図されない。オーサリング鍵(CED)を使用する際には、コンテンツID(CID)とオーサリング鍵使用鍵(CEK)が分かれば、モジュール内部でKcidを生成することにより、オーサリング鍵(CED)に含まれるコンテンツ鍵(Kc)、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)、コンテンツ使用可能化鍵のバージョン情報(EKB-Version)を獲得することができる。

【0121】(2.3.2 情報配信端末400において使用される鍵情報および鍵関連情報) 情報配信端末400においては、暗号化コンテンツデータの(E(Kc, Content))復号時、外部認証時、内部認証時に、それぞれ鍵情報および鍵関連情報が使用される。

【0122】(復号時に使用される情報)「暗号化コンテンツデータ(E(Kc, Content))」は、デバイス鍵(Kdevice)およびコンテンツ使用可能化鍵(EKB)、第2のコンテンツ鍵(EKc)から獲得されるコンテンツ鍵(Kc)を利用して復号化される。

【0123】「デバイス鍵(Kdevice)」は、パッケージ化されたコンテンツを利用可能な再生装置に関する鍵情報である。デバイス鍵は、各再生装置がハードウェア的にあるいはタンパレジスタントソフトにより、セキュアに保持している鍵情報である。

【0124】「コンテンツ使用可能化鍵(EKB)」は、ルート鍵(Kroot)をデバイス鍵(Kdevice)で暗号化したものである。コンテンツ使用可能化鍵(EKB)には、E(KdeviceA, Kroot), E(KdeviceB, Kroot)といったデータが格納されており、再生装置A(DeviceA)は、E(KdeviceA, Kroot)を解くことに

(15)

特開2009-69548

27

よりKrootを知ることが可能である。同様に、再生装置B (DeviceB) は、E (KdeviceB, Kroot) を解くことによりKrootを知ることが可能である。

【0125】(外部認証時に使用される鍵情報) 情報提供部420の外部認証時には、第1の外部認証鍵(Kauth(1))と第2の外部認証鍵(Kauth(2))が使用される。

【0126】「第1の外部認証鍵(Kauth(1))」は、認証サーバ部500から事前に、情報提供部420に配布される外部認証鍵である。この第1の外部認証鍵(Kauth(1))は、情報提供部420の認証部(セキュアモジュール)内にタンパレジスタント(Tamper Resistant)に隠蔽されているので、リバースエンジニアリングしても値を調べることは困難である。第1の外部認証鍵(Kauth(1))は、第1の暗号化手段4224が乱数を暗号化して第1の暗号化データを生成する際に用いられる。

【0127】「第2の外部認証鍵(Kauth(2))」は、認証サーバ部500により発行される第1の外部認証鍵(Kauth(1))と同一の鍵である。第2の外部認証鍵(Kauth(2))は、第2の暗号化手段4225が乱数を暗号化して第2の暗号化データを生成する際に用いられる。

【0128】(内部認証時に使用される鍵情報) 情報提供部420の内部認証時には、情報提供部420とリーダー/ライター490とがそれぞれ有するデバイス鍵(Kdevice)でコンテンツ使用可能化鍵(EKB)を復号して得られたルート鍵(Kroot)が参照される。

【0129】(2.4 ユーザ部) ユーザ部180は、キオスク端末などの情報配布端末400にアクセスし、気に入ったコンテンツをダウンロードする機能を有しているコンピュータ装置などの情報処理端末である。

【0130】ユーザ部180は、図1に示すように、メモリスティックなどの記憶媒体182と再生装置184を主な構成要素としている。さらに、ユーザ部180は、他の記憶媒体および/または再生装置186を備える場合もあり、許可された回数内で、記憶媒体182にダウンロードしたコンテンツを、他の記憶媒体および/または再生装置186に対して、チェックアウトまたはムーブすることが可能である。

【0131】(3 オーサリング動作) 次に、オーサリングスタジオ300におけるオーサリング動作について説明する。本実施の形態にかかる情報配信システム100においては、オーサリング時にコンテンツの暗号化とパッケージ化を行うこと、およびオーサリング鍵を生成するオーサリング鍵生成装置160と実際にオーサリング鍵を用いてコンテンツの暗号化を行うオーサリング装置316とを別構成にしたこと、さらに、ルート鍵を直接オーサリング装置316に渡さずにコンテンツの暗号

28

化を可能にしたことなどを特徴としている。

【0132】また、オーサリングを行う際に、オーサリング鍵の内容は知る必要が無いため、オーサリング鍵の生成とオーサリング作業を完全に分離することが可能である。さらに、オーサリング作業とオーサリング鍵生成を分離することにより、オーサリング作業で正しく生成できるパッケージの数を、オーサリング作業の外で制御することが可能である。

【0133】さらに、オーサリング鍵生成時に使用する暗号化の鍵として、コンテンツ識別子(CID)に加えてオーサリング鍵生成時に任意に指定できるオーサリング鍵使用鍵(CEK)を付加することにより、生成したオーサリング鍵を正しく使用できる人をオーサリング鍵使用鍵(CEK)を知っている人に限定することができる。

【0134】さらに、オーサリング時に設定した、利用条件等の内容に対して、正しいシステムのみ知り得る鍵を使用したMAC値を付加することにより、パッケージの改ざんを防止することができる。

【0135】(3.1 オーサリング鍵の生成動作) オーサリング鍵生成装置(鍵管理装置)180におけるオーサリング鍵の生成動作について説明する。

【0136】オーサリング鍵(CEK)には、基本的には、コンテンツ鍵(Kc)、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)の情報が含まれる。なお、EKcは、E(Kroot, Kc)と表現することが可能である。また、ルート鍵(Kroot)は、コンテンツ鍵(Kc)を暗号化するために使用される鍵であり、セキュリティのために非常に重要な鍵である。後述するように、本システムによれば、共通に使用されるルート鍵(Kroot)をオーサリング装置316に直接渡すことなく、コンテンツ鍵(Kc)、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)のセットをオーサリング鍵(CEK)としてオーサリング装置316に渡すことにより、セキュリティを向上させるとともに、組み合わせの間違いを防止することができる。

【0137】図17(1)に示すように、オーサリング鍵(CEK)は、コンテンツデータを暗号化するためのコンテンツ鍵(Kc)とルート鍵で暗号化した第2のコンテンツ鍵(EKc)を、コンテンツデータ毎にユニークに割り当てられるコンテンツ識別子(CID)とオーサリング装置316毎にユニークに割り当てられるオーサリング鍵使用鍵(CEK)で暗号化したものである。

【0138】図6に示すオーサリング鍵生成手段166において、オーサリング鍵(CEK)の生成に必要なものは、コンテンツ識別子生成手段182により生成されたコンテンツ識別子(CID)と、コンテンツ鍵(Kc)と、ルート鍵(Kroot)で暗号化したコンテンツ鍵(EKc)と、オーサリング鍵使用鍵生成手段164によりオーサリング鍵使用鍵(CEK)である。



【0139】図16に、オーサリング鍵生成手段166において実施されるオーサリング鍵(CED)の生成工程の詳細なフローを示す。

【0140】まず、ステップS1602において、オーサリング鍵(CED)の中に含まれるべき、コンテンツ鍵(Kc)、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)、コンテンツ使用可能化鍵のバージョン情報(EKB-Version)を連結し、さらに不正な解読を困難とするために冗長な乱数情報を付加したデータブロックである、冗長コンテンツ鍵ブロック(RKcB (Redundant Kc Block))を生成する。

【0141】なお、コンテンツ使用可能化鍵(EKB)は、ルート鍵(Kroot)をデバイス鍵(Kdevice)で暗号化したものであり、コンテンツ使用可能化鍵のバージョン情報(EKB-Version)は、コンテンツ使用可能化鍵のバージョン情報である。このように、あるコンテンツ鍵(Kc)に対して特定されるべきルート鍵(Kroot)のバージョン(Version)を示す情報をもセットにすることにより、コンテンツ鍵(Kc)、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)、ルート鍵(Kroot)の組み合わせの間違いを防ぐことができる。

【0142】次いでステップS1604において、冗長コンテンツ鍵ブロック(RKcB)のチェックサム(CS)を計算し、例えば、チェックサム(CS)を冗長コンテンツ鍵ブロック(RKcB)の後ろに連結することによりチェックサム付冗長コンテンツ鍵ブロック(CRKcB)を獲得する。

【0143】このようにオーサリング鍵(CED)を生成する過程において、コンテンツ鍵(Kc)とルート鍵で暗号化した第2のコンテンツ鍵(EKc)以外にチェックサム情報を負荷することにより、誤ったコンテンツ識別子(CID)によるオーサリング鍵(CED)による使用を非常に高い確率で防止することができる。

【0144】次いでステップS1608において、コンテンツ識別子(CID)とオーサリング鍵使用鍵(CEK)から最終暗号化鍵(Kcid)を生成する。図17(2)に関連して後述するように、オーサリング鍵(CED)を使用する際には、コンテンツID(CID)とオーサリング鍵使用鍵(CEK)が分かれば、モジュール内部でKcidを生成することにより、オーサリング鍵(CED)に含まれるコンテンツ鍵(Kc)、ルート鍵で暗号化した第2のコンテンツ鍵(EKc)、コンテンツ使用可能化鍵のバージョン情報(EKB-Version)を獲得することができる。

【0145】ここで、最終暗号化鍵(Kcid)を生成する過程において、コンテンツ毎にユニークなコンテンツ識別子(CID)を使用することにより、オーサリング鍵による暗号化作業の際に、正しいコンテンツ識別子

(CID)を使用した場合に正しいオーサリング作業が可能となるので、オーサリングの精度を高めることが可能となる。また、コンテンツ識別子(CID)の生成を、オーサリング鍵生成装置160において管理することにより、コンテンツ識別子(CID)のユニーク性を完全に保証することができる。

【0146】最後にステップS1608において、チェックサム付冗長コンテンツ鍵ブロック(CRKcB)を最終暗号化鍵(Kcid)で暗号化することによりオーサリング鍵(CED)を生成する。

【0147】(3.2 オーサリング鍵による暗号化動作) 次に、図18を参照しながら、オーサリング鍵生成装置(鍵管理装置)160において生成されたオーサリング鍵によるコンテンツの暗号化動作について説明する。

【0148】まずステップS1902に示すように、オーサリング装置316のコンテンツ鍵復号化手段3162は、オーサリング鍵生成装置(鍵管理装置)160から共有秘密鍵であるオーサリング鍵使用鍵(CEK)を取得する。なお、以下において、オーサリング鍵を生成するオーサリング鍵生成装置とオーサリング鍵などの鍵情報を管理する鍵管理装置を同一の装置として説明するが、オーサリング鍵生成装置と鍵管理装置とは別体に構成しても構わない。

【0149】次いで、ステップS1904において、コンテンツ鍵復号化手段3162は、オーサリング鍵生成装置(鍵管理装置)160からオーサリングするコンテンツ用にコンテンツ識別子(CID)とオーサリング鍵(CED)のペアを取得する。

【0150】ステップS1902およびS1904に関して、オーサリング鍵(CED)は、コンテンツ識別子(CID)とオーサリング鍵(CED)のペアと同じタイミングで取得する必要は無い。コンテンツ識別子(CID)とオーサリング鍵(CED)のペアはコンテンツ毎に異なるが、オーサリング鍵使用鍵(CEK)はオーサリング装置316にユニークな値なので、オーサリング処理に先立って一度取得しておけばよい。

【0151】また、コンテンツ識別子(CID)とオーサリング鍵(CED)のペアに関しても、各コンテンツをオーサリングする度にその都度取得する必要はない。複数のコンテンツをオーサリングする場合には、一括取得するように構成しても構わない。

【0152】次いで、ステップS1906において、コンテンツ鍵復号化手段3162は、図17(2)に示すように、オーサリング鍵(CED)から、コンテンツ識別子(CID)とオーサリング鍵使用鍵(CEK)を用いて、コンテンツ鍵(Kc)とルート鍵で暗号化した第2のコンテンツ鍵(EKc)とを復号化する。

【0153】次いで、ステップS1908において、オーサリング装置316のコンテンツ暗号化手段3164

は、コンテンツ鍵復号化手段3162により復号化したコンテンツ鍵(Kc)を用いてコンテンツデータを暗号化して暗号化コンテンツデータE(Kc, Content)を生成する。

【0154】次いで、ステップS1910において、パッケージ手段3166により、暗号化コンテンツデータE(Kc, Content)とともに、コンテンツ識別子(CID)とルート鍵で暗号化した第2のコンテンツ鍵(EKc)とをパッケージ化して一連のオーサリング作業を終了する。

【0155】(4 情報配信動作) 以上のようにしてオーサリング処理が終了したコンテンツは、図1に示すように所定のネットワーク600を介してキオスク端末などの情報配信端末400に送信される。情報配信端末400には、図19に示すように、暗号化コンテンツ(E(Kc, Content))、ルート鍵で暗号化されたコンテンツ鍵(EKc)およびコンテンツ使用可能化鍵(EKB)が送られる。なお、暗号化コンテンツE(Kc, Content)のヘッダ部には、改ざん防止用に、コンテンツ鍵Kcを用いて計算したMAC値が付加される。

【0156】情報配信端末400においては、外部認証および内部認証から成る所定の認証動作が完了した後に、復号化処理がなされ、所定の記憶媒体182にダウンロードが行われる。以下、図20に示すフローに沿って情報配信動作の詳細について説明する。

【0157】(4.1 外部認証動作) すでに説明したように、情報配信端末400の外部認証部422は、情報提供部420が正規のものであるか、すなわち情報配布端末400が記憶しているコンテンツを外部に提供する権限を有するかどうかを、情報提供部420が予め保管する第1の外部認証鍵(Kauth(1))と、認証サーバ500が保管する第2の外部認証鍵(Kauth(2))とを用いて、比較認証する(ステップS2102)。ステップS2102において、外部認証に成功すれば、ステップS2104以下において行われる内部認証に進むが、外部認証に失敗すれば、コンテンツの情報配信(DL)動作は拒絶される(ステップS2112)。

【0158】外部認証は、情報提供部420を起動するたびに必ず行う必要がある。ただし、一度認証が通れば、情報提供部420の起動中は再度行わなくてもよい。

【0159】なお外部認証は、要求されるセキュリティレベルに応じて、第2の暗号化手段4225による第2の暗号化データ取得の態様を変更することにより、さまざまな実施形態を採用可能である。

【0160】(4.1.1 ローカル外部認証動作) 最もセキュリティレベルが低い実施形態は、図18に示すように、ローカルで、すなわち情報提供部420内にお

いて外部認証を行う。この実施形態においては、第2の外部認証鍵(Kauth(2))が情報提供部420内のアプリケーション内に組み込まれている。

【0161】まず第1の外部認証鍵(Kauth(1))をセキュアに保持するセキュアモジュール425は、乱数発生手段4223により生成した乱数を第1の外部認証鍵(Kauth(1))により暗号化し、第1の暗号化データを得る。

【0162】乱数発生手段4223により発生された乱数は、アプリケーションインタフェース423を介してアプリケーション421に送られる。アプリケーション421は、予め記憶している第2の外部認証鍵(Kauth(2))を用いて乱数を暗号化し、第2の暗号化データを得る。

【0163】第2の暗号化データは、アプリケーションインタフェース423を介して、セキュアモジュール425に戻される。セキュアモジュール425内において、第1の暗号化データと第2の暗号化データとが比較され、両者が一致した場合に、本実施の形態にかかる外部認証作業が終了する。

【0164】しかしながら、かかるローカル外部認証の態様では、情報配布端末400を悪意に操作する者に第2の外部認証鍵(Kauth(2))が盗まれる可能性がある。また情報配布端末400自体を盗まれた場合には、情報配布端末400内に記憶されたパッケージのダウンロードが可能になってしまう。

【0165】(4.1.2 リモート外部認証動作) これに対して、最もセキュリティレベルの高い実施形態は、図14に示すように、リモートで、すなわち情報提供部420の外部にある認証サーバ500を利用して外部認証を行う。

【0166】まず第1の外部認証鍵(Kauth(1))をセキュアに保持するセキュアモジュール425は、乱数発生手段4223により発生した乱数を第1の外部認証鍵(Kauth(1))により暗号化し、第1の暗号化データを得る。

【0167】乱数発生手段4223により発生された乱数は、アプリケーションインタフェース423、アプリケーション421を介して認証サーバ部500に送られる。認証サーバ部500は、認証サーバ部500内に上記乱数を取り込んで、第2の外部認証鍵(Kauth(2))を用いて第2の暗号化データを生成する。

【0168】第2の暗号化データは、アプリケーションインタフェース423を介して、セキュアモジュール425に戻される。セキュアモジュール425内において、第1の暗号化データと第2の暗号化データとが比較され、両者が一致した場合に、本実施の形態にかかる外部認証作業が終了する。

【0169】このように本実施の形態にかかる外部認証動作によれば、第2の外部認証鍵(Kauth(2))

が盗まれることがなく、また情報配布端末400自体を盗まれた場合であっても、情報配布端末400内に記憶されたパッケージのダウンロードを行うことはできない。

【0170】(4. 1. 3 セミローカル外部認証動作)さらに、図13に示す実施形態と図14に示す実施形態との中位のセキュリティレベルを有する実施形態を図15に示す。この実施形態においては、認証サーバ部500は、必要に応じて、例えばダウンロードを行う際に、第2の外部認証鍵(Kauth(2))を情報提供部420に一時的に受け渡される。

【0171】まず第1の外部認証鍵(Kauth(1))をセキュアに保持するセキュアモジュール425は、乱数発生手段4223により発生された乱数を第1の外部認証鍵(Kauth(1))により暗号化し、第1の暗号化データを得る。

【0172】乱数発生手段4223により発生された乱数は、アプリケーションインタフェース423介してアプリケーション421に送られる。アプリケーション421は、予め記憶している第2の外部認証鍵(Kauth(2))を用いて乱数を暗号化し、第2の暗号化データを得る。

【0173】ここで、第2の外部認証鍵(Kauth(2))は認証サーバ部500が管理しており、情報提供部420を起動する度に、アプリケーション421は認証サーバ部500から第2の外部認証鍵(Kauth(2))を受け取り、乱数に対して暗号化処理を行う。第2の暗号化データが生成された後に、あるいは情報配布端末400への電源が遮断されることに、第2の外部認証鍵(Kauth(2))は情報提供部420から消去される。

【0174】第2の暗号化データは、アプリケーションインタフェース423を介して、セキュアモジュール425に戻される。セキュアモジュール425内において、第1の暗号化データと第2の暗号化データとが比較され、両者が一致した場合に、本実施の形態にかかる外部認証作業が終了する。

【0175】この実施形態によれば、ダウンロードなどの必要な時にのみ、第2の外部認証鍵(Kauth(2))が情報配布端末400に一時的に受け渡されるので、第2の外部認証鍵(Kauth(2))自体の盗難の可能性が著しく軽減される。また情報配布端末400自体を盗まれた場合であっても、第2の外部認証鍵(Kauth(2))が情報配布端末400の電源を遮断した時点で消去されてしまう構成を採用すれば、情報配布端末400内に記憶されたパッケージのダウンロードを行うことはできない。

【0176】(4. 2 内部認証動作)内部認証部424による内部認証動作は、情報提供装置420の外部認証完了後に行われる。内部認証動作は、第1の認証手段

4242によって行われるコンテンツの検証動作(第1の認証動作)と、第2の認証手段4244によって行われる第2の認証動作とから構成されている。

【0177】図20のステップS2104に示すコンテンツの検証動作は、配布対象であるコンテンツデータが、正規のオーサリングシステム(オーサリングスタジオ300)により作成されたコンテンツであるかを検証するための手段を提供する。具体的には、第1の認証は、正規のオーサリングシステムが前記コンテンツデータに書き込んだMAC(Message Authentication Code)を参照して行われる。ステップS2104において、コンテンツの検証に成功すれば、ステップS2106において行われる第2の内部認証に進むが、コンテンツの検証に失敗すれば、コンテンツの情報配信(DL)動作は拒絶される(ステップS2112)。

【0178】ステップS2106において、第2の認証手段4244は、記録手段であるリーダー/ライター430と情報記録管理手段である情報提供装置420との相互認証を行うための手段を提供する。第2の認証手段4244は、まず、正規のオーサリングシステム300が、ルート鍵(Kroot)をデバイス鍵(Kdevice)で暗号化したコンテンツ使用可能化鍵(EKB)を、リーダー/ライター430と情報提供装置420との双方に受け渡す。リーダー/ライター430と情報提供装置420は、それぞれがセキュアに保持するデバイス鍵(Kdevice)を用いてルート鍵(Kroot)を復号化させる。そして、復号化されたルート鍵(Kroot)が相互に一致する場合に肯定的な認証を行う。ステップS2106において、第2の内部認証に成功すれば、ステップS2108においてダウンロードが許可されるが、第2の内部認証に失敗すれば、コンテンツの情報配信(DL)動作は拒絶される(ステップS2112)。

【0179】(4. 3 ダウンロード動作)以上のようにして、図20に示すステップS2106において内部認証が完了した後に、ステップS2206において、メモリスティックなどの所定の記憶媒体にコンテンツをダウンロードする。

【0180】以下、図22を参照しながら、内部認証、復号化処理、ダウンロード処理の連携関係について詳細に説明する。

【0181】まずデバイス鍵(KdeviceA)をセキュアに保持する情報提供装置420は、ダウンロード対象のパッケージのMAC値をチェックして、ダウンロード対象のパッケージが正規のオーサリングシステムにより作成されたものであり改ざん等がされていないことを確認する。

【0182】情報提供装置420は、パッケージに含まれるコンテンツ使用可能化鍵(EKB)をデバイス鍵

(KdeviceA)で復号してルート鍵(KrootA)を取得する。情報提供装置420は、コンテンツ使用可能化鍵(EKB)をリーダ/ライタ430に送信する。リーダ/ライタ430も、情報提供装置420と同様に、デバイス鍵(KdeviceB)をセキュアに保持している。リーダ/ライタ430は、情報提供装置420から受け取ったコンテンツ使用可能化鍵(EKB)をデバイス鍵(KdeviceB)で復号化して、ルート鍵(KrootB)を取得する。

【0183】情報提供装置420とリーダ/ライタ430は、双方のルート鍵(KrootA, KrootB)を比較し、第2の内部認証を行う。

【0184】内部認証に成功すると、さらにコンテンツの正当性をチェックしてから、リーダ/ライタ430により、メモリスティックなどの記憶媒体にコンテンツをコピーする。

【0185】この段階では、コンテンツはまだコンテンツ鍵(Kc)により暗号化されており、再生は不可能である。そこで、コンテンツ鍵(Kc)を用いて、コピーしたコンテンツを再生制御装置により再生可能状態にすることにより、ユーザは、自己所有の再生装置184によりコンテンツを楽しむことが可能となる。

【0186】(4.4 複数コンテンツの一括ダウンロード動作)図22に示す例では、一つのコンテンツをコピーする例を示したが、本実施の形態にかかる情報配布システムにおいては、複数のコンテンツを同時にダウンロードすることも可能である。

【0187】図23を参照しながら、複数コンテンツの一括ダウンロード動作について説明する。所定の認証動作が成功した後に、情報提供装置420は、リーダ/ライタ430を介して、所定の記憶媒体182に対して、第1のパッケージをコピーする。この段階では、第1のパッケージにかかるコンテンツの再生は不可能である。次いで、情報提供装置420は、リーダ/ライタ430を介して、所定の記憶媒体182に対して、第2および第3のパッケージをコピーする。このようにして、複数のコンテンツの一括ダウンロードが完了すると、再生制御装置は、ダウンロードが完了した複数のコンテンツをまとめて再生可能状態にする。

【0188】このように、ダウンロードする度に1曲1曲再生可能にするのではなく、例えば3曲のダウンロード要求に対して3曲書き込んだ後に3曲分一括に再生可能にすることにより、複数のコンテンツを一括ダウンロードする際の認証等の手間を大幅に軽減することができる。

【0189】(4.5 ダウンロード後のコンテンツの流れ)次に図24を参照しながら、本実施の形態にかかる情報配布システムによりダウンロードしたコンテンツのその後の流れについて説明する。

【0190】図24に示すように、本システムによ

ば、キオスク端末(情報配信装置)400から一旦メモリスティックのような記憶媒体にパッケージ化されたコンテンツはダウンロードされる。パッケージ内には、コンテンツの利用条件に関する情報も含まれており、この条件に従って、ダウンロード後のコンテンツの処理方法が決定される。

【0191】通常は、メモリスティックなどの記憶媒体182からパーソナルコンピュータなどの端末装置190にコンテンツをインポートする。そして、端末装置190から再び再生機能を有する携帯機器192, 194, 196にコンテンツをチェックアウトすることが可能である。チェックアウトの回数は、著作権保護のために、制限されており、図示の例では、3回のチェックアウトが許可されている。したがって、3種類の携帯機器192, 194, 196に対してダウンロードしたコンテンツをコピーすることが可能である。

【0192】チェックアウト回数を超えて、上記携帯機器192, 194, 196以外の再生装置にコンテンツをコピーしたい場合には、いずれかの携帯機器192, 194, 196から一旦コンテンツをパーソナルコンピュータ190にチェックインした後に、許可されたチェックアウトの回数内でコピーすることが可能となる。

【0193】以上説明したように、本実施の形態にかかる情報配信システムによれば、オーサリング時点でコンテンツを暗号化しているの、情報配信端末側でのダウンロード時間を短縮し、情報配信端末側の負荷を軽減することができる。

【0194】本実施の形態にかかる情報配信システムによれば、情報配信端末側では、正規のオーサリング装置で作成したコンテンツしかダウンロードできないように制限をかけているので、オーサリング後に中身を一部手で書き換えるといったような不正行為を防止できる。また不正にオーサリングしたコンテンツを情報配信端末に持ってきてもそのコンテンツをダウンロードすることができない。

【0195】本実施の形態にかかる情報配信システムによれば、正規のコンテンツであっても、単純に記憶媒体にコピーしただけでは再生可能にはならない。再生可能にするには、情報提供装置側において外部認証および内部認証が必要となるため、不正コピーを防止できる。

【0196】本実施の形態にかかる情報配信システムによれば、正規購入したコンテンツファイルは何回でもダウンロード可能であり、また正規にダウンロードしたコンテンツファイルをPCに移動させ、PCと他の装置との間でチェックアウト/チェックインすることができる。

【0197】本実施の形態にかかる情報配信システムによれば、楽曲ファイルなどのメインコンテンツ以外にも、ジャケット写真等の付随データもメインコンテンツに関連付けて処理することができる。

【0198】以上、添付図面を参照しながら本発明にかかる情報配信システム等の好適な実施形態について説明したが本発明はかかる例に限定されないことは言うまでもない。当業者であれば、特許請求の範囲に記載された技術的思想の範疇内において、各種の変更例または修正例に想到し得ることは明らかであるが、それらについても当然に本発明の技術的範囲に属するものと了解される。

【0199】例えば、上記実施形態においては、本発明にかかる情報配信システム等の好適な実施形態として、当該システムを音楽データを配信用コンテンツとして配信するシステムに適用した場合について説明したが、本発明はかかる例に限定されない。例えば、当該システムは、音楽データ以外にも、画像（静止画および動画を含む）データ、ゲームプログラムなどの様々なコンテンツデータをネットワークを介してユーザに対して配信する情報配信システムにも適用可能であることはいうまでもない。

#### 【0200】

【発明の効果】以上説明したように、本発明によれば、不正なコピーを有効に防止して楽曲データなどの配信することが可能な情報配信システムを構築できる。すなわち、本発明によれば、オーサリング時の不正操作、配信時の不正操作、情報配信端末の不正操作、ダウンロード時の不正操作を有効に防止することが可能である。さらに、本発明によれば、オーサリング時に圧縮および暗号化を行うので、ダウンロードに時間がかからない情報配信システムを構築することが可能である。

#### 【図面の簡単な説明】

【図1】本発明の実施の一形態にかかる情報配信システム100の概略構成を示すブロック図である。

【図2】本発明の実施の一形態にかかる情報配信システム100のコンテンツホルダ120の概略構成を示すブロック図である。

【図3】本発明の実施の一形態にかかる情報配信システム100のコンテンツアグリゲータ200の概略構成を示すブロック図である。

【図4】本発明の実施の一形態にかかる情報配信システム100のオーサリングスタジオ300の概略構成を示すブロック図である。

【図5】本発明の実施の一形態にかかる情報配信システム100におけるオーサリングスタジオ300ののオーサリング部310の概略構成を示すブロック図である。

【図6】本発明の実施の一形態にかかる情報配信システム100のオーサリングシステムにおけるオーサリング装置316とオーサリング鍵生成装置160との関係の概略構成を示すブロック図である。

【図7】本発明の実施の一形態にかかる情報配信システム100のオーサリングシステムの構築例を示すブロック図である。

【図8】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400の概略構成を示すブロック図である。

【図9】本発明の実施の一形態にかかる情報配信システム100の情報提供部420の概略構成を示すブロック図である。

【図10】本発明の実施の一形態にかかる情報配信システム100の情報提供部420の外部認証部422の概略構成を示すブロック図である。

10 【図11】本発明の実施の一形態にかかる情報配信システム100の情報提供部420の内部認証部424概略構成を示すブロック図である。

【図12】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400のシステム構成例を示すブロック図である。

【図13】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400において行われる外部認証（ローカル）の一例を示すブロック図である。

20 【図14】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400において行われる外部認証（リモート）の一例を示すブロック図である。

【図15】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400において行われる外部認証（セミローカル）の一例を示すブロック図である。

【図16】本発明の実施の一形態にかかる情報配信システム100のオーサリング鍵生成工程を示すフローチャートである。

【図17】本発明の実施の一形態にかかる情報配信システム100のオーサリング鍵生成工程を示す説明図である。

【図18】本発明の実施の一形態にかかる情報配信システム100のオーサリング工程を示すフローチャートである。

【図19】本発明の実施の一形態にかかる情報配信システム100の配信対象である暗号化コンテンツ（E（Kc, Content））、ルート鍵で暗号化されたコンテンツ鍵（EKc）およびコンテンツ使用可能化鍵（EKB）の構成を示す説明図である。

40 【図20】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400における情報配信工程を示すフローチャートである。

【図21】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400におけるコンテンツ復号工程を示すフローチャートである。

【図22】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400におけるパッケージのダウンロード工程を示すフローチャートである。

50 【図23】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400における複数のパッケージを一括してダウンロードするダウンロード工程を示す

(21)

特開 2003-69548

38

40

すフローチャートである。

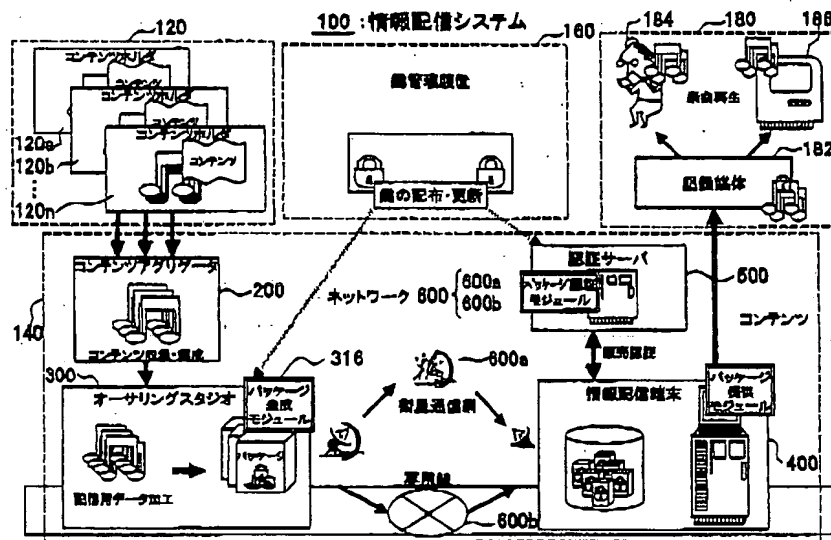
【図24】本発明の実施の一形態にかかる情報配信システム100の情報配信端末400において一旦ダウンロードしたコンテンツのその後の処理について示す説明図である。

【符号の説明】

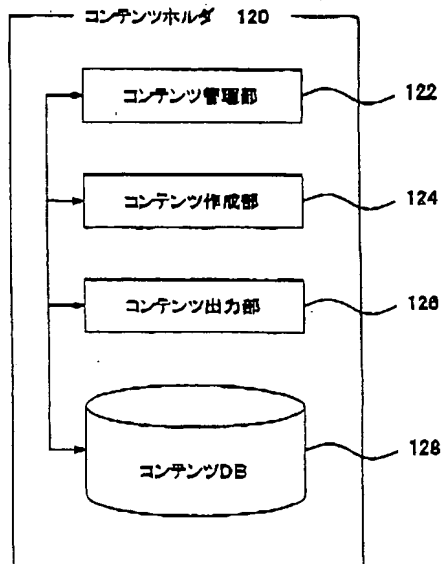
100 情報配信システム  
120 コンテンツホルダ

140 コンテンツ流通部  
160 鍵管理装置（オーサリング鍵生成装置）  
180 ユーザ  
200 コンテンツアグリゲータ  
300 オーサリングスタジオ  
400 情報配信端末（キオスク端末）  
500 認証サーバ  
600 ネットワーク

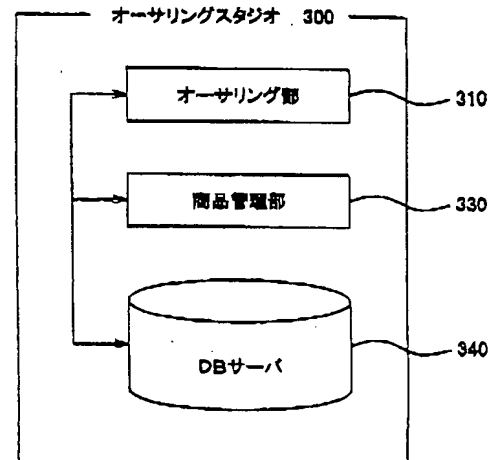
【図1】



【図2】



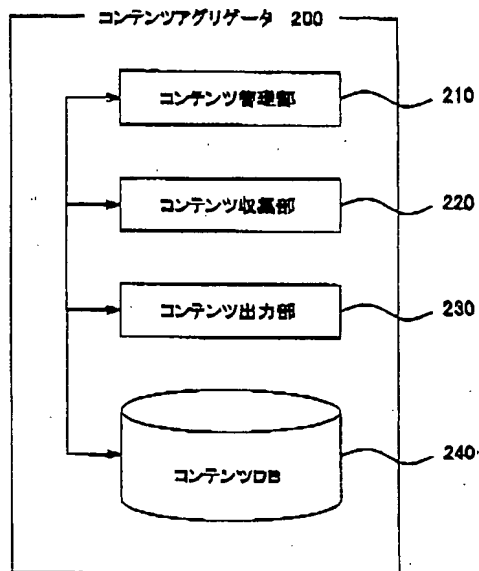
【図4】



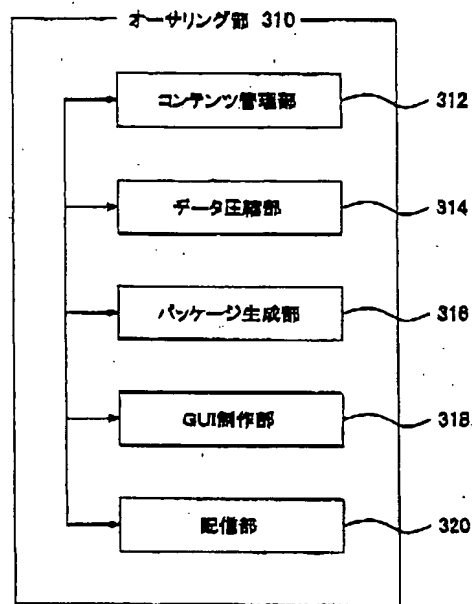
(22)

特開 2003-69548

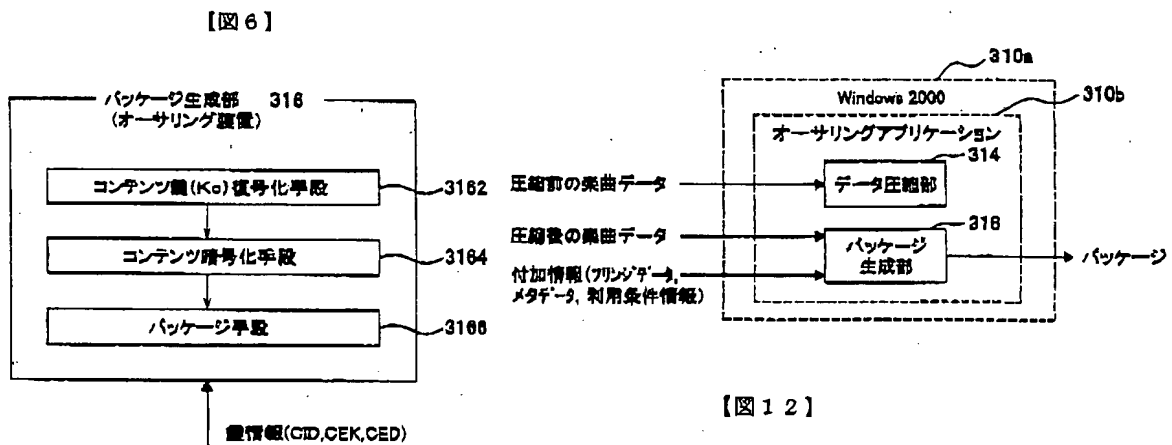
【図3】



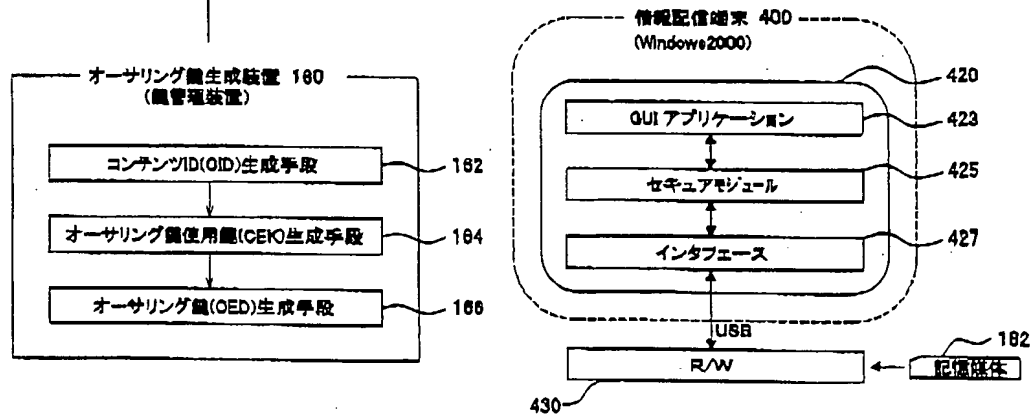
【図5】



【図7】



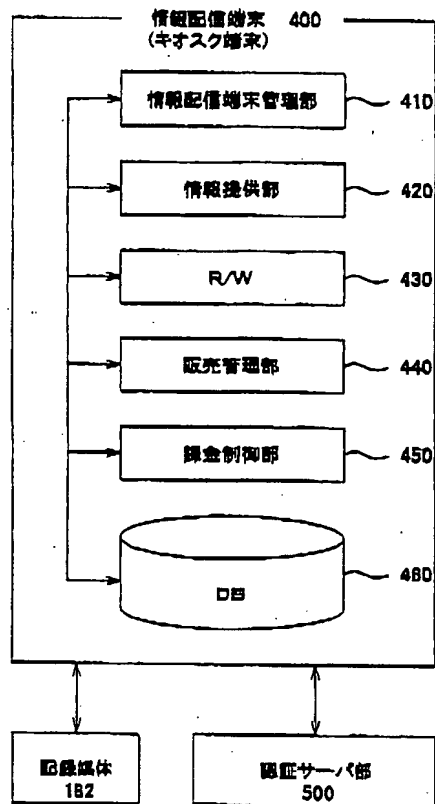
【図12】



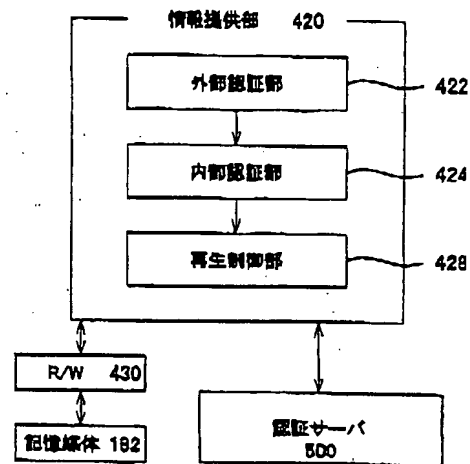
(23)

特開 2003-69548

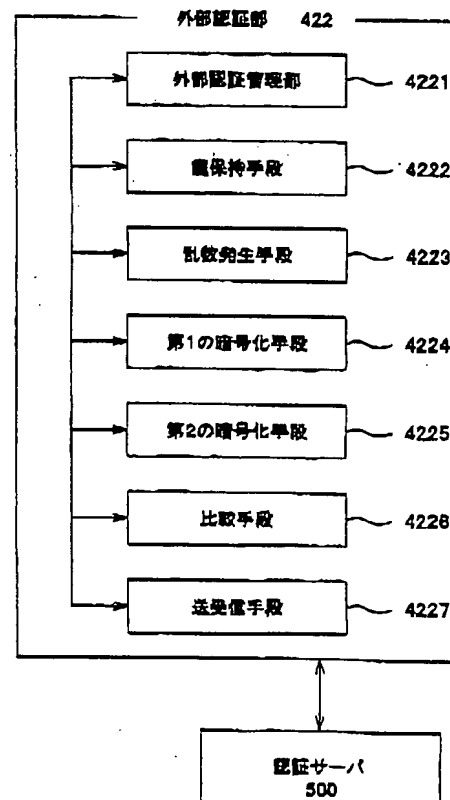
【図 8】



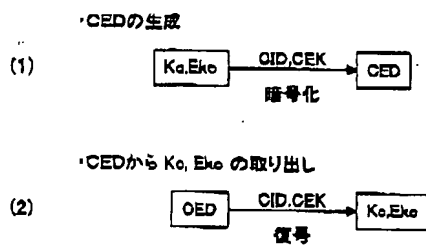
【図 9】



【図 10】



【図 17】

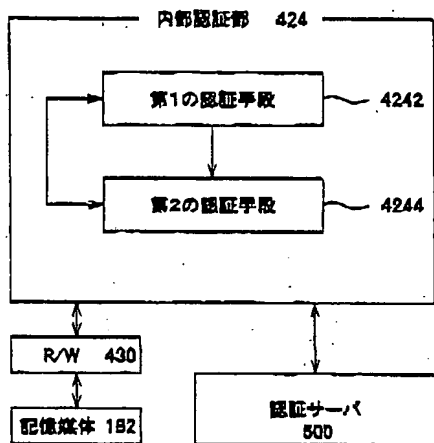




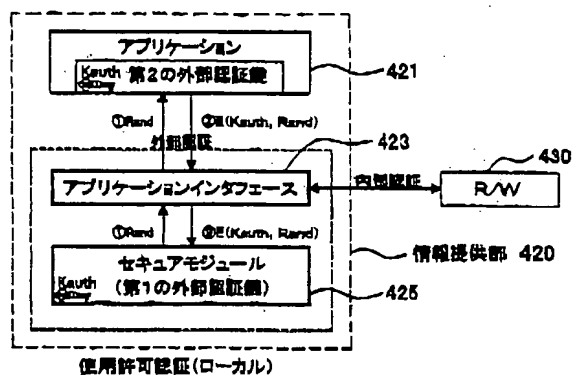
(24)

特開 2003-69548

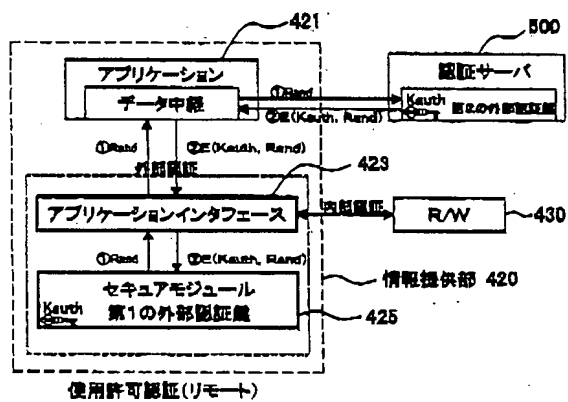
【図 11】



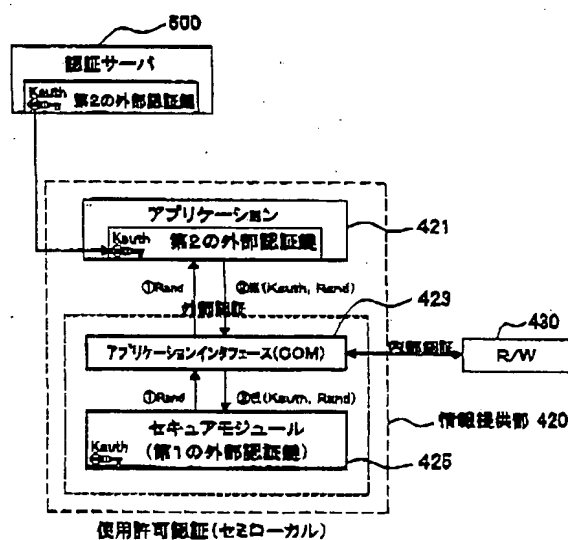
【図 13】



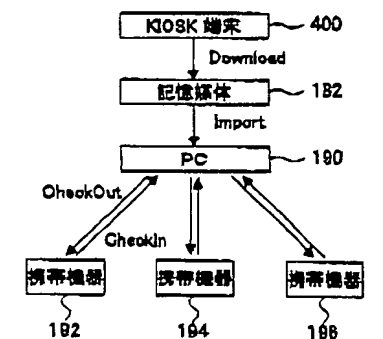
【図 14】



【図 15】



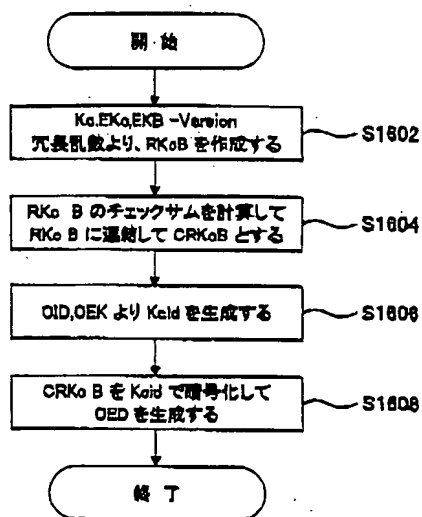
【図 24】



(25)

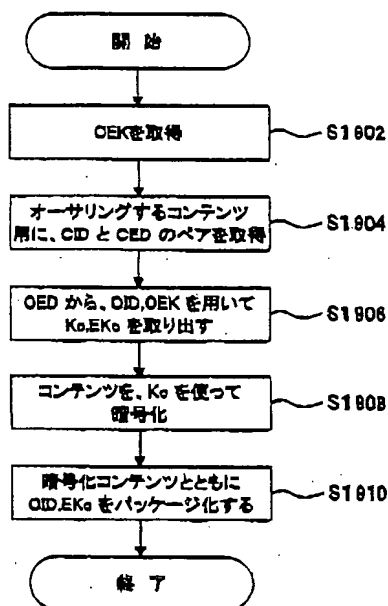
特開2003-69548

【図16】



OED作成フロー

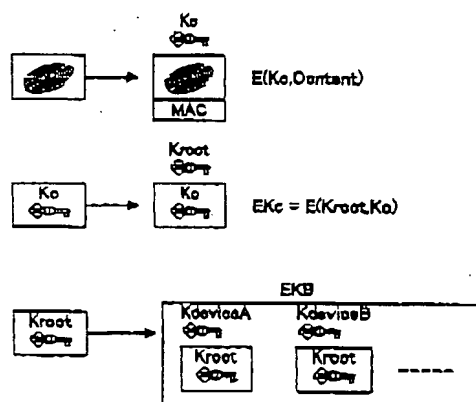
【図18】



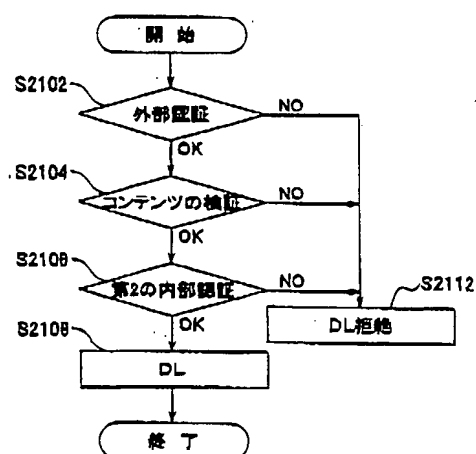
オーサリングフロー

【図19】

コンテンツの暗号化, Eke の生成, EKB の生成



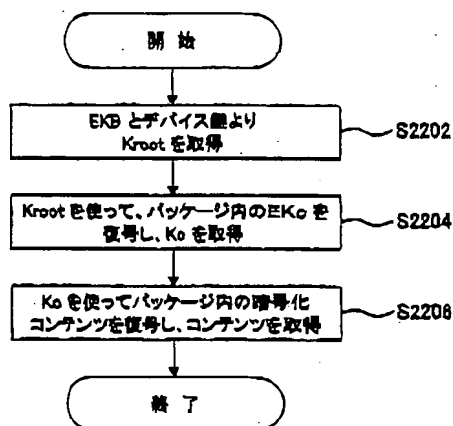
【図20】



(26)

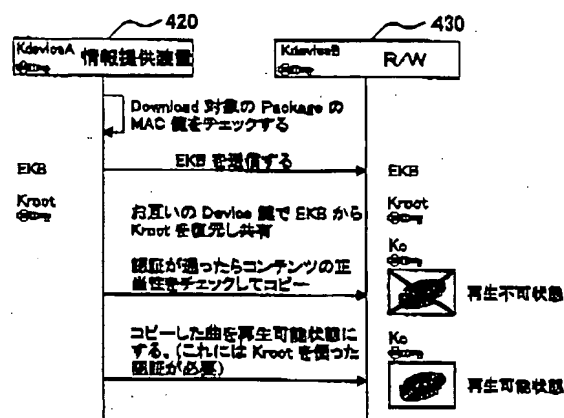
特開 2003-69548

【図 21】



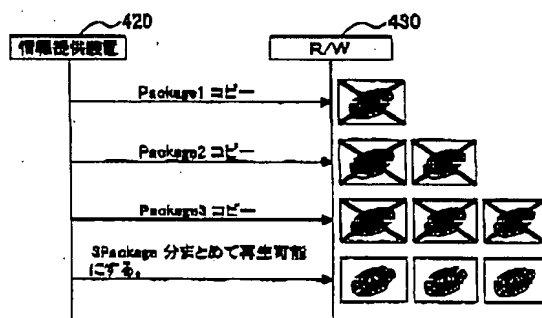
コンテンツ復号フロー

【図 22】



パッケージのダウンロードの流れ

【図 23】



複数パッケージのダウンロード

フロントページの続き

(72)発明者 上野 信一  
東京都品川区北品川 6 丁目 7 番35号 ソニ  
ー株式会社内

F ターム(参考) 5B085 AA08 AE29  
5J104 AA01 AA13 AA16 EA04 EA26  
NA02

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**